9-1-2005

Third National Transportation Security Summit: Rail Security – A Symposium onTerrorism and Business Continuity, MTI Report s-05-02

MTI

MTI REPORT S-05-02

THIRD NATIONAL TRANSPORTATION SECURITY SUMMIT: RAIL SECURITY—A SYMPOSIUM ON TERRORISM AND BUSINESS CONTINUITY

SEPTEMBER 29, 2005

April 2006

a publication of the
Mineta Transportation Institute
College of Business
San José State University
San José, CA 95192-0219

Created by Congress in 1991

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA/CA/OR-2006/25		

4. Title and Subtitle	5. Report Date
Third National Transportation Security Summit: Rail Security—A Symposium on Terrorism and Business Continuity	April 2006
	6. Performing Organization Code

7. Authors	8. Performing Organization Report
Symposium	MTI S-05-02

9. Performing Organization Name and Address	10. Work Unit No.
Mineta Transportation Institute College of Business San José State University	11. Contract or Grant No. 65W136

12. Sponsoring Agency Name and Address		13. Type of Report and Period
California Department of Transportation Sacramento, CA 95819	U.S. Department of Transportation Research and Innovative Technology Administration 400 7th Street, SW Washington, DC 20590-0001	Final Report 14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

This event is one in a series of research and information transfer symposia on transportation security best practices presented by the National Transportation Security Center (NTSC) at the Mineta Transportation Institute (MTI). The symposium was held in conjunction with the American Public Transportation Association (APTA) Annual Meeting in Dallas, Texas, on September 29, 2005.

With a focus on operational security and business continuity for rail transportation systems in the event of terrorist act or cataclysmic natural disaster, this one-day symposium brought together transportation, security, emergency response, and business continuity management experts.

Symposium presenters included Brian Michael Jenkins, Jeanne Lin, Dr. Frances L. Edwards, and Mortimer Downey, III. A panel presention moderated by Mr. Downey, which included Greg Chilson, Greg Hull, Ron Hynes, and Jo Strang, offered lively discussion about such topics as crisis management, security practices and policies, and recommendations for making rail transportation more robust and secure.

17. Key Words	18. Distribution Statement
Hazards and emergency operations; Passenger security; Rail transit facilities; Terrorism; Transportation facilities	No restrictions. This document is available to the public through the National Technical Information Service, Springfield, VA 22161

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	112	$15.00

Form DOT F 1700.7 (8-72)

Library of Congress Catalog Card Number: 2006925151

To order this publication, please contact the following:
Mineta Transportation Institute
College of Business
San José State University
San José, CA 95192-0219
Tel (408) 924-7560
Fax (408) 924-7565
E-mail: mti@mti.sjsu.edu
http://transweb.sjsu.edu

ACKNOWLEDGMENTS

The Mineta Transportation Institute thanks the following individuals and organizations for their assistance in planning and presenting the *Third National Transportation Security Summit: Rail Security—A Symposium on Terrorism and Business Continuity*, which was held on September 29, 2005 in Dallas, Texas, in conjunction with the American Public Transit Association's Annual Meeting and Conference.

We thank each of our presenters and panelists for making the time in their busy schedules and for flying into the face of a hurricane to share their knowledge and expertise: George Chilson, Mortimer Downey, Frances Edwards, John Horsley, Greg Hull, Ron Hynes, Brian Jenkins, Jeanne Lin, and Jo Strang. No less committed and courageous were the many representatives of public and private agencies and transportation systems who also weathered the storm to contribute to this discussion.

We thank our co sponsors: the American Association of Railroads, the American Association of State Highway and Transportation Officials, the American Public Transit Association, the Federal Railroad Administration, the Federal Transit Administration, the National Association for Railroad Passengers, the National Railroad Passenger Corporation (Amtrak), and the Transportation Security Administration of DHS.

Special recognition must be given to the liaisons from each of the sponsor organizations. These dedicated individuals served as expert advisors to help plan the event and set the agenda: Leo Penne, AASHTO; Greg Hull, APTA; Barry Warner, Amtrak; Michael Tabor, FTA; Ross Capon, NARP; Chris McKay and Don Thompson, TSA; all worked diligently with MTI staff, including Executive Director Rod Diridon, Communications Director Leslee Hamilton, and Research Director Trixie Johnson, in the planning of this event.

Successful implementation of this event was accomplished through the leadership and support of William Millar, Executive Director, APTA, and the highly professional team responsible for planning and staging the 2005 APTA Annual Meeting and Conference.

MTI would also like to recognize the following staff members for their contributions to both the program and to this document: Sonya Carter, Publications Assistant; Barney Murray, Web Administrator; Pam Bishop and Shun Nelson, Graphic Designers, with logistics support from Brendan McCarthy, Latora Gardner, Heather Gornitzka and Saldy Suriben. Editing and publication services were provided by Catherine Frazier. We especially thank James Swofford for being the project manager of this symposium and editor of this publication.

TABLE OF CONTENTS

LIST OF FIGURES

FOREWORD

Attacks against rail transportation systems worldwide demonstrate terrorists' continued interest in using trains as a means for inflicting physical and psychological harm. Additionally, natural disasters similarly ripped the fabric of transportation systems along the U.S. Gulf Coast, even as this meeting was taking place. These events illustrate the complexity of returning those systems to service after a cataclysmic incident.

The Third National Transportation Security Summit, conducted by the National Transportation Security Center at the Mineta Transportation Institute, featured a one-day symposium on Rail System Security and Business Continuity on September 29, 2005 to coincide with the American Public Transportation Association (APTA) Annual Meeting in Dallas, Texas.

For over a year prior to this, a planning committee with liaisons representing each of the cosponsoring organizations conferred and determined that the focus should be on business continuity. Furthermore, the presidential order requiring implementation of the National Incident Management System (NIMS) presents specific challenges to executives with Emergency Operations Center (EOC) responsibilities. Lack of (or improper) training and certifications in conformance with the NIMS requirements may expose unprepared organizations to legal liability.

This discussion of those topics provided updated information to policy makers, rail transportation executives, and to security and first-responder managers who are responsible for restoring operational and business activities as quickly and securely as possible after a terrorist incident or natural disaster.

This publication is an abridged account of the proceedings. It is edited for continuity by removing incidental asides and personal acknowledgements. It also is desensitized to make sure that there is nothing in it that would help those intent on causing harm. All of the MTI/NTSC case studies referenced herein, and a chronology of all the terrorist attacks since 1920, are also available on *TransWeb*, the MTI website, in a desensitized format.

Rod Diridon, Sr.

Executive Director

EXECUTIVE SUMMARY: THE THIRD NATIONAL TRANSPORTATION SUMMIT: RAIL SECURITY—A SYMPOSIUM ON TERRORISM AND THE BUSINESS COMMUNITY

Operational security and business continuity for rail transportation systems in the event of a terrorist act or cataclysmic natural disaster were the focus of this one-day symposium, which featured presentations and a roundtable discussion by experts in transportation, security, and emergency preparedness.

This event is one in a series of research and information transfer symposia on transportation security best practices presented by the National Transportation Security Center (NTSC) at the Mineta Transportation Institute (MTI). The symposium was held in conjunction with the American Public Transportation Association (APTA) Annual Meeting in Dallas, Texas, on September 29, 2005.

John Horsley, MTI Board Chair and Executive Director of the American Association of State Highway Transportation Officials (AASHTO) opened the symposium. Mr. Horsley established the framework for the summit and set the scope of the following discussions. Speaking of lessons learned through past experiences—from the September 11, 2001 terrorist attacks to Hurricane Rita, which made landfall the day before the meeting—he observed that the needed response for both types of events is virtually the same. Mr. Horsley challenged the participants to develop integrated planning methods and communications systems, and the appropriate levels of response, so as not to unnecessarily amplify the economic impacts of an incident. He also challenged the federal government to find the funds needed to support those efforts.

Making white paper presentations were leading experts on transportation, safety, and security.

Brian Michael Jenkins, Director, MTI National Transportation Security Center and one of the world's leading authorities on terrorism and counterterrorism, presented "The Changing Threat," a definition and redefinition of jihadists' worldwide terrorism. Mr. Jenkins discussed case studies on recent terrorist acts against rail transportation systems in London, Madrid, and elsewhere.

Jeanne Lin, Director, Border and Transportation Security Portfolio, U. S. Department of Homeland Security Science & Technology Directorate, presented "Security Strategies for

Mass Transit," an overview of DHS organizations, programs, resources, and strategies for rail transportation security.

Author, educator, and emergency management professional Dr. Frances L. Edwards, Research Associate, MTI National Transportation Security Center, presented "Implementing NIMS." She discussed federal requirements for transportation and emergency-response managers who are responsible for implementing the National Incident Management System (NIMS). She described resources available from MTI and other sources that will help these managers achieve compliance.

Mortimer Downey, III, Chairman, PB Consult, Inc., presented "Business Continuity Management," featuring insights honed as the chief operating officer at U.S. DOT. Mr. Downey developed the agency's highly regarded strategic and performance plans and had program responsibilities for operations, regulation and investments in land, sea, air, and space transportation. He described business continuity issues that rail transportation and emergency preparedness managers must consider when confronted with terrorism or severe natural disasters.

Mr. Downey then moderated a panel discussion and a question-and-answer session with the audience followed. The expert panel included participants representing varied points of view: George Chilson, President of the National Association of Railroad Passengers (NARP); Greg Hull, Director of Operations, Safety and Security Programs for APTA; Ron Hynes, Deputy Associate Administrator, Office of Research, Demonstration and Innovation, Federal Transit Administration (FTA); and Jo Strang, Deputy Associate Administrator for Railroad Development, Federal Railroad Administration (FRA). In the discussion that followed, national, state, and local emergency management professionals from the United States and Canada explored:

- Crisis management—public and private responsibilities and partnerships
- Security practices and policies—evolving trends and technology implementations
- Recommendations for making rail transportation more robust and secure.

Co-sponsors for this event were the American Association of Railroads (AAR), American Association of State Highway Transportation Officials (AASHTO), American Public Transportation Association (APTA), Federal Railroad Administration (FRA), Federal Transit Administration (FTA), National Association of Railroad Passengers (NARP), National Railroad Passenger Corporation (Amtrak), and the Transportation Security Administration (DHS/TSA).

INTRODUCTION

ROD DIRIDON:

The intent of this discussion is for you who are on the firing line to be able to share your thoughts with some of the experts in the field of security and emergency response, especially in regard to business continuity.

We are finding from our research and from comments from those in positions of responsibility who are attending to the natural disasters over the last month that business continuity is much more of a problem than we had expected in the past. We have been distracted by concerns about security, and those are terribly important, but we also have to devote more attention to the process of developing National Incident Management System (NIMS) plans and to exercising those plans in a manner that will allow us to get back to work after a security event or a natural disaster.

We will begin by introducing the chair of the Mineta Transportation Institute's Board of Trustees, and the Executive Director of the American Association of State Highway and Transportation Officials, AASHTO, and that is John Horsley.

JOHN HORSLEY:

This is the Third National Transportation Security Summit. The second was held just 40 days after September 11, 2001 and was jointly sponsored by the Mineta Transportation Institute, the American Public Transportation Association (APTA), and the American Association of State Highway and Transportation Officials (AASHTO). We thought it was important to bring national experts like Brian Jenkins to the table to talk with transit and highway leaders from all over the country in those first few weeks after 9/11, so we convened that event. The Mineta Institute has continued to increase its expertise beyond that it had achieved leading up to that terrible day in America's history. But think about what has happened since then; the attack in Madrid took place in 2004; the attack on the London subway system has taken place this year (2005). I think the questions on our minds today could be: "Who is next; where is next?"

Also, we may ask: "Have we done enough, since 9/11, to position rail managers, transit managers, and transportation managers to be ready to respond?"

Unfortunately, from the experiences during Hurricanes Katrina and Rita, we do not seem to have learned a great deal. If there is anything that I would point to from the lessons of Hurricane Katrina it is that we are all in it together. When you have police, fire, federal, state, and local officials, one of the things to take away from an event like this is how important it is to network, plan, exercise, prepare, and think more broadly than we do generally.

I represent all 50 state departments of transportation. One of our frustrations since the attack of 9/11 is that the state DOT's have received virtually no capital assistance, no financial assistance whatsoever, from the federal government to help us do a better job as first responders. We had the Secretary of Transportation from Alabama, Mississippi, and Louisiana at the AASHTO annual meeting in Nashville, Tennessee, and one of the featured points of frustration they expressed was the communications breakdown during the hurricanes. When an event of such magnitude happens, communications are fundamental for all levels of government to be able to talk to each other, and certainly we have to address that. But in order to do it, we need our federal partners up and down the line to help us address that in terms of policy and resources.

We have another concern now that the Transportation Security Administration (TSA) and the Federal Emergency Management Administration (FEMA) have been taken away from their previous homes and assigned exclusively to the Department of Homeland Security. We do not have the same integration of decision making and understanding of the role that transportation plays in either anticipating or responding to a terrorist attack or responding to a natural disaster. We have lost the integrated thinking and the assessment and understanding of the dynamics.

If one side of a coin represents the threat from terrorism and the other side represents the threat from a natural disaster, the response that we need to be prepared to deliver in either eventuality is the same. There are some different preventive measures, but the emergency response that we need in place is virtually the same protocol for either case.

Finally, we must remember the broader implications. Osama Bin Laden and his followers had no idea of the ripple effects to the national economy that their attack on the World Trade Center (WTC) would cause, but it was in the billions of dollars because of both the reaction and the overreaction that took place. As a national response protocol, we need to understand that we should not amplify the impacts on our economy and the American people by underplanning, underpreparation, and inappropriate overreaction.

I think that all of those are lessons we have learned in the last four years.

THE CHANGING THREAT

Presentation by Brian Michael Jenkins, Director, National Transportation Security Center

Figure 1 Brian Michael Jenkins

JOHN HORSLEY:

The Mineta Transportation Institute is a superb national resource located at San José State University. One of the featured services provided by the institute is the National Transportation Security Center (NTSC) run by Brian Michael Jenkins, and it is my pleasure at this time to introduce him.

Brian Jenkins is one of the world's leading authorities on terrorism and sophisticated crime. He served with distinction in the U.S. Army as a Captain in the Green Berets, with service in the Dominican Republic and several tours of duty in Vietnam. He received

Bachelor of Arts and Master of Arts degrees from the University of California at Los Angeles (UCLA) and was a Fulbright Fellow working with the Organization of American States stationed in Mexico and Guatemala.

In 1996, President Clinton appointed him to serve on the White House Commission on Aviation Safety and Security. For much of his career, he was chairman of the Political Science Department at the Rand Corporation, where he directed their research in political violence.

BRIAN MICHAEL JENKINS:

Since 9/11, we have seen how terrorists are focusing on public transportation systems in a variety of ways. Even before the events in London—the bombings on July 7, 2005, and the attempted bombings on July 21, 2005—there were revelations of a plot that the police had uncovered to contaminate the Heathrow Express with chemical weapons. There have been a number of terrorist attacks on trains and subways in Russia, and another bomb on a ferry in the Philippines.

Since the beginning of 2004, there have been a number of major attacks that have killed about three hundred persons on trains and subways. As of September 2005, about 142 persons have been killed and more than 3,000 people injured. So we are not talking about something that is theoretical here; we are talking about something that is a continuing demonstration of terrorists' interest in attacking public transportation, surface transportation systems.

Some of the observations that I am offering here are based upon continuing research that the Mineta Transportation Institute has been doing for over ten years now. The bulk of this focuses on specific case studies.

When we first began looking at this, we did not have a rich history of major terrorist attacks on our transportation systems. Other countries, unfortunately for them, did so our efforts were focused on looking at those actual cases of attacks on systems to distill lessons learned and to identify the best practices that we might apply.

There is a philosophical assumption that the kind of security model that we have in place for commercial aviation in the United States is not going to work for public surface transportation. That model is a mandated, highly regulated, rule-based security system that must, given the nature of our aviation system, be uniform across the country. When I was on the White House Commission, I learned that we have 430 commercial airports in

this country, with around 700 million aviation passengers boarding each year. We must have a system that provides uniform protection throughout. It makes no difference whether you board an airplane in the District of Columbia or in Duluth, Minnesota, the system has to be the same, and it is rule based.

When we look at our public surface transportation system in this country, it is quite different. It is vast, with 6,000 different systems including everything from huge, urban multimodal systems to small, rural bus systems. The threat varies across the country. Security is provided by proprietary police departments in some cases, by private security in some cases, and by local law enforcement. The idea that we could apply one set of rules to this diverse system simply is not going to work.

Moreover, there is the issue of the delays that would be involved. While it may be acceptable to wait in line for 15 to 20 minutes, in some cases longer, in an airport to board an airplane for a cross-country flight, no one is going to wait in line for half an hour to get on a subway to take a 15-minute ride.

As for manpower requirements, we have about 45,000 people assigned to airport security and passenger screenings to deal with the 700 million boardings. If we look at rail and bus together, there are about 20 billion passenger boardings in this country. We would need hundreds of thousands of screeners. If we add the costs to screen trains and buses, we are going to destroy public surface transportation; it is not going to work.

Instead, we have to use a best practices approach. That is where we distill the lessons learned from actual cases, provide a menu of security practices, and then enable the individual operators to select from that menu to come up with the best combination of security measures that are appropriate to their particular system and circumstances. For the past ten years, MTI has conducted case studies of terrorism against transportation systems and we have some preliminary results from those studies.

Why do terrorists go after surface transportation targets? Because from the terrorists' perspective, they are attractive; they provide easy access. Because they are public transportation, they are designed to provide easy access, and, therefore, they also provide easy escape. These are congregations of strangers, guaranteeing the attackers anonymity. And, of course, all of these attacks cause great alarm and disruption.

It is clear from our chronology of these attacks that terrorists who go after transportation systems often seek slaughter. Two-thirds of these attacks are intended to kill and indeed about 40 percent of them do result in fatalities. This is compared to about 20 to 25 percent

of terrorist attacks overall, so they produce almost twice the fatalities. When they go after public transportation, they are not making a symbolic gesture. These are not the equivalent of the terrorist bomb in front of the embassy at midnight. The attacks are intended to kill people; they do succeed, and indeed multiple fatalities are often the consequence. Every attack in the past two years has been intended to kill. This is not symbolic terrorism; this is lethal terrorism.

Terrorists may calculate that for the kind of bomb that they can make and smuggle onto a rail system, their return is going to be about 15 to 20 fatalities per bomb. Attacks are almost equally distributed between bus systems and rail systems.

Bombings are the most common form of attack. The various kinds of bombs that are carried on, thrown at, or set off inside transportation systems amount to about 64 percent of the terrorists' tactics.

When we look at the number of other kinds of attacks that have been tracked over the years, we see that the terrorist threat is focused against people, for the most part, and not against infrastructure. To look at this from the perspective of the terrorists, if you have so many individuals, so much explosive, and so much expertise, are you going to take on a big, tough target like a bridge, or are you going to get a guaranteed return in terms of fatalities by going after people? We know they are fascinated by the idea of big targets, because we look at their plans. We know that they have conducted reconnaissance. They are fascinated with bridges and tunnels. These targets keep recurring in their thinking, but they are not easy targets because they are robust structures. Therefore, the terrorists tend to return to going after people instead of going after the infrastructure of a system.

When we talk about roads, there are different issues. Both public transportation systems or roads and highways become the lifelines for moving people out of harm's way, as well as for getting emergency crews and reinforcements into the right locations. That is a vital role in any large scale evacuation or any major effort in delivering emergency personnel and equipment.

They worked very well on 9/11 in New York. At the moment of impact, when the first plane hit the tower, there were thousands of passengers in Lower Manhattan on trains, in the tunnels, in the stations immediately below the World Trade Center and in the adjacent Battery Park, along with hundreds more Metropolitan Transportation Authority (MTA) employees. Every single passenger and employee was moved out of the way without a single casualty underground; that worked very, very well.

We saw further evidence of good work when mobilizing the bus system. In fact, they used the plan that they had originally crafted to deal with evacuating the city as a consequence of a possible hurricane. They took that plan and made it into a new plan very quickly to get people out of Lower Manhattan. Using what they call a "load and go" protocol, they moved people off the island. As those trains returned, they brought firemen and police from outside the city to ground zero. All of that worked extremely well.

I think that was important for the nation because, had we seen in New York on 9/11 the kind of breakdown that we saw in the wake of Hurricane Katrina, it would have contributed to a sense of national panic. It was not just that it worked well in New York, it is that we all watched it. The fact that it was working well was an important thing in reducing some of the terror that the terrorists hoped to create.

There were some problems in getting people out of Washington, D.C., on 9/11. The federal government closed down and sent everybody home. There were problems coordinating between the District of Columbia and the surrounding states' departments of transportation. Highways were jammed; buses that carried people out of Washington could not get back in. Some of the problems then were the same problems underscored later during the evacuations in the hurricanes.

Now let us turn to some of the lessons that we are learning from particular case studies. These are described in detail in a series of Mineta Transportation Institute publications that have these specific case studies described in detail, with the lessons learned and best practices identified.

The 25-year terrorist campaign against surface transportation in England, by today's standards, was a comparatively innocent campaign. The Irish Republican Army, in pursuit of its political agenda, was certainly willing to kill, but did have certain self-imposed constraints. If things became too bloody, financial contributions and support for the IRA went down in Ireland, the United States, and elsewhere. They had to gauge their determination to use violence against some loss of potential constituents if it became too bloody. So, the IRA campaign was a much more controlled one. In all transportation systems, 17 persons were killed and 200 injured. But it was an intense campaign in the 1990s; at its peak, there were 81 explosive devices on London Transport. On trains in Southern England, over 6,000 bomb threats, and 9,000 suspicious objects were dealt with by police. The number of abandoned parcels investigated was in the many thousands.

The utility of all those incidents, however, is that the volume allowed analysis. It is very hard to do analysis about response and perfecting security measures if you are dealing with

statistically rare events. This is a common problem in security. If you are dealing with a problem like shoplifting, you can measure it daily; computers can tell you the inventory shrinkage. You can put into place a new security system, such as cameras or electronic tags, and you can identify the results and calculate them out to the second decimal place. If you are dealing with rare events, it is very difficult to say what is affected and what is working.

Because there has not been another attack on the United States since 9/11, does that mean we are doing exactly the right thing; or does it mean another attack is being planned and we will find out about it some time from now? What conclusions we draw from that are very difficult to discern.

The IRA campaign did allow us to identify the adversary's *modus operandi* and to gauge the effect of security measures and determine what measures worked. As security was increased in the heart of London, the IRA was pushed back from some of its very high profile targets, like the Victoria Station, to stations in outer London. As the security measures moved out, the IRA was pushed out even further until finally, near the end of the campaign, they were blowing up switchboxes on outskirts.

We also were able to see that the government, by providing information and constant exhortations to the public, did actively engage the public in the security process. In fact, they could depend on being warned within minutes of discovery of a suspicious left object. They had extensive use of closed-circuit television to aid in identifying those incidences and providing quick response. One lesson learned is when we should engage the public. This is a judgment call, for it may alarm people and scare them off the system. On the other hand, engaging the public does provide a lot of potentially useful information. However, simply exhorting people to be alert has no use unless there are readily accessible, well-marked communication systems for individuals to communicate something. Just telling them to be alert does not do it.

Beyond the communications systems, there has to be rapid, visible response. If there is communication from the public and nothing happens, the people stop communicating. For example, I remember being in an airport just after 9/11 and seeing an unattended suitcase that was sitting there for 15 minutes. I finally walked up to the person at the desk and I told them that suitcase has been sitting there for 15 minutes with nobody connected to it. Their response was they were really busy and they did not have time for that. That is not the way you enlist the public into the security effort. There has to be a system, not just an exhortation to be alert.

Now we look at the Tokyo incident where the terrorists used sarin, a nerve gas, during the morning rush hour. The trains were moving along; some people were getting off and getting sick because of the fumes, other people were jamming on, and as the trains go to the next station, more people stagger off, not feeling well from the effects of the gas, as others are pushing their way onto the trains.

Diagnosis was very difficult; the train system operators simply did not know what was going on. They did not have the camera coverage or the information gathering systems to tell them what was happening. As a consequence, one of the contaminated trains went all the way through downtown Tokyo to the end of the line, reversed, and came back through the city again, doing the same thing—spilling out sick passengers, taking on new passengers, going to the end of the line and reversing a second time. It was on its third passage before the train finally was stopped, an hour and 40 minutes later. In addition, some of the station staff picked up the little bags of sarin from the floor and carried them to trashcans. One of those individuals died because of the exposure to sarin. Others would have died except for the slight measure of protection provided by the white gloves that the station people wear in Tokyo.

About 5,500 people were treated at hospitals. They had real symptoms: breathing problems, vomiting, and asthma attacks. Of those people, about 1,200 had actually been exposed to nerve gas. The other people were in distress with symptoms, but their distress was caused by panic, not by the nerve gas. One thing you can depend on in these circumstances is that the number of casualties you will be treating will vastly exceed those who were, in fact, exposed to the chemical or radioactive element used.

As I mentioned in the 9/11 case study, with surface transportation, the lesson learned was that crisis management plans, supported by regular tabletop and field exercises, were critical. All of the things that you expect to happen in a catastrophe did occur in New York. Because of the first World Trade Center bombing in 1993, there was a strong urge to maintain a level of preparedness. Unfortunately, the brand new office for the emergency center that they built was in Building 7 at the World Trade Center, and so that was lost right away. Communications went out—no command center, no communications. How did people respond to this? They responded by doing what they had done in the exercises and modified their plans on the fly. You can depend on communications going out, and you can depend on losing touch with emergency centers, but because this had been practiced, drilled in tabletop exercises, people did what they had done before, and things managed nonetheless to work.

Now, some preliminary lessons learned from Madrid. First of all, why did they do it? Al-Qaeda propaganda about Spain being part of the historic Muslim world certainly signaled an attack. There had been some other attempts by the Euskadi Ta Askatasuna (ETA) Basque separatists to carry out bombings on the rail system. That is a good clue for those involved in rail security. If you have a highly publicized event in some part of the world, whether it succeeds or not, it is the right time to take your security up a notch, because it is going to give other folks ideas. One event sets off thinking about future events.

We are still not certain that they planned to affect the outcome of the elections. That just may have been a collateral benefit that they picked up along the way. We know that the planning for this act began sometime in late 2002 or early 2003. It was a long time in planning, but the specific operation itself was put together in three months in 2004.

They knew the system. They had good information. It was not hard to get; they could just ride the trains. They planned the attack to the minute, but they were foiled a bit by the fact that, uncharacteristically, one of the trains was a couple of minutes late and that prevented another train from pulling into the station. This may have saved a significant number of lives because, if all of the bombs went off in the station itself, the casualties may have been much greater. Clearly, the attacks were intended to kill, because the design of the bombs was meant to rip people apart.

We are not sure if they did trial runs because some of the principal conspirators killed themselves rather than be captured by Spanish police when they were tracked down several days later. However, we do know that they did not travel far with their assembled bombs. The bombs were actually put together and armed at the last minute in a van near where they boarded the trains. This is also characteristic and not surprising. Terrorists do not like to take long rides with bombs ready to go, particularly bombs that are going to be set off by a cell phone call—a wrong number, and they are gone and these guys were not suicidal.

As for warnings, there were no warnings for Madrid; there was no prior chatter indicating something was up. Perhaps the propaganda should have been taken as a warning. The publicity surrounding the thwarted ETA attack should have been taken as a warning. What we are still investigating is that apparently there was a partially assembled bomb found the day before, which may have been an indicator. The issue is, if you have mechanisms in place, you can get the word around very quickly about an assembled bomb and quickly increase security.

Now, here are some preliminary observations from the London attacks. As we get into the London attacks, I want to underscore the word "preliminary" and advise you that this is a work in progress. I do not want it to sound as if we are armchair analysts criticizing the failures of the British system here because this is all still preliminary.

The attacks probably were inspired by Madrid and by having a number of prior plots that the police knew about that had involved public transportation. However, there were no specific indicators of this cell. In fact, three weeks before the July 7 attack, intelligence had reported there was nothing specific on the horizon. It was completely beneath their radar.

We did learn that closed-circuit television is not going to deter suicide attackers. They do not care if they have their picture taken. However, it did provide a tremendous help in permitting the rapid identification of the bombers, which led to confirmation that it was a suicide attack. This was a source of relief because it showed they were not dealing with a situation like Madrid where there were still some terrorists at large. The ones who did this were killed in the process of doing it.

It may have accelerated action by the second cell that carried out the attack on July 21, which was not as bad. Their hasty planning may have resulted in the faulty attack.

The response was excellent; coordination was excellent, again reflecting lots of practice. Random search procedures were accepted by the public. However, the shoot-to-kill policy which was in place for dealing with suicide bombers (which is in place in many locations) certainly became controversial after the death of a young Brazilian.

On the morning of July 7, unconnected with the terrorist attack, there had been a major mechanical failure and another mechanical failure where smoke was coming out of one of the locomotives and it had to be replaced. And in yet another incident, there was a failure with a train's brakes that had resulted in a temporary shutdown. When the first bomb went off, it was read initially as a power surge that had short-circuited the system. There was no direct communications with the trains in the tunnels that there was an explosion. One of the early reports was that a suicide had resulted in a derailment of the train. It was when people came out of the tunnels and the emergency responders saw they were blast casualties that they knew it was not just a derailment. The diagnosis was a problem. I am not saying that had their reaction time been faster, more lives would have been saved. Indeed, if more bombs were already in the system, bringing trains to the station was not necessarily going to change that.

There was almost a total communications failure. The existing police radio sets did not communicate in the deeper tunnels. The police, and a lot of other people, used their own cell phones. But the minute this incident took place, the whole London cell phone system was flooded with millions of calls. The system went down not because of damage; it went down because of volume abuse. The police were handling a huge volume of information. Some of it was simply wrong: a suicide creating derailments; there was an explosion. A lot of it was rumor. As you can imagine, every package that was anywhere was reported. Suddenly, the police were flooded with calls. One of the things that they are thinking about is how they can create an information cell that will handle high volumes of information and sort out what is actually going on. That is a major challenge in these instances. The people in London are pretty good about adjusting to things; they had a lot of experience with the IRA campaign, but the challenge was to get them some kind of information about what was going on, and there were problems in being able to do that.

Getting people home without the public transportation system working was a concern. It was a nice, sunny July day, so a lot of people walked home. Had it been midwinter, that would not have worked. There are real issues with how you move people out of a city when you lose your public transportation system.

There are some questions about how, despite the heightened security, a second cell on July 21, 2005 was still able to penetrate. Interestingly enough, in terms of psychological effects, people responded pretty well to the July 7 bombing. But when the second attempt took place, it rattled the public because it suggested that there is a second, or possibly a third terrorist, cell.

There was a bomb on a bus an hour after the initial attack. The fellow on the bus did not plan for that bomb to go off on the bus. He was supposed to get into a station and onto a train. That was supposed to be a fourth bomb on the train. We do not know all the details yet, but we know that he was not able to get on the train. We know that he made a number of cell phone calls to his mates, trying to call them, but by that time, they were already dead. He then got on that bus. What we do not know is if he decided then that he was going to carry out his bombing on a bus because he could not get into a train station, which had all been sealed. Some eyewitness accounts say that he was fiddling with the device. We do not know if he had second thoughts and was trying to disarm it, but the bomb went off. I like to think that he had second thoughts. But what we know is that he was supposed to be on a train.

What is interesting is that we know now the July 21 bombers were not directly connected with the July 7 bombing. On July 21, they tried to replicate the July 7 attack, including three on the train, and one on the bus, not realizing that the one on the bus was a mistake. That tells us that they were not in touch, but two separate cells.

All of this underscores the fact that the threat is real. We are dealing with people who use very long planning horizons to put their final operation together. We know that they remained determined to carry out the attacks. Our presumption has to be that they are going to continue to try to carry out attacks and certainly surface transportation is in their playbook. We know that attacks on public surface transportation are more likely than attacks on infrastructure. We know that these large scale attacks put major burdens on roads and traffic control systems, especially those that result in transportation system shutdowns. We know they thought about bridges and tunnels in 1993, when they thought about the Brooklyn Bridge. We know that they have attacked in Paris.

There was the 1997 "Flatbush Plot," where in New York self-starting jihadists were going to use suicide vests to carry out bombings on the subway system. One of the conspirators got nervous about it and went to a couple of transit cops. In barely comprehensible English, he actually persuaded them that there was something going on. Instead of dismissing the guy as a nut, they took it seriously and interrupted a serious terrorist plot.

We know from plans that have been discovered, they want to carry out attacks on transportation targets in Singapore, Manila, Milan, and Moscow. We know that they see Madrid as a great success. We know that an attack was planned in New York in 2004 by a couple of locals of Pakistani origin. The plot was not a mature plot and was picked up by police intelligence. Because the Republican National Convention was coming to New York, they could not keep these guys under surveillance and run the risk that they might lose them and, heaven forbid, something would occur. So, they moved in early and picked them up.

We see the threat coming at us from several different directions. We may have locals operating entirely on their own, as was the case in the 1997 and 2004 plots in New York, and clearly the case for the 2005 attacks in London. Or there may be recruits sent in to reconnoiter targets and plan operations as we have seen examples of that with Iyman Faris looking at the Brooklyn Bridge. Also, they might think about attacks assisted from abroad, as was the case in 1993 World Trade Center bombing. Less likely are foreign teams inserted into the country, which was the 9/11 scenario. The operational environment for

that is very difficult for them now, so we are seeing more neighborhood al-Qaedas and much more decentralized operations.

Let me quickly touch upon some axioms about security. First, it is very difficult to quantify the terrorist threat and, therefore, determine the right level of security. How much security is enough is a really tough question. cost/benefit analysis does not work well here. What we do know is that security does work and that it does drive people away from their preferred targets. On the other hand, if you are at the federal government level, or thinking about investing in security, you have to look for a net security benefit. One of the problems we have in protecting public places is that there are lots of public places. We can draw a perimeter of security around any public place and we can secure that piece of geography, but it does not stop the terrorist attacks; it simply moves them down the street. We can be selfish about that and say that our responsibilities are for surface transportation—we will deal with this particular problem—but the net security benefit is a consideration.

There are some desirable attributes of surface transportation security. One is the ability to increase and decrease security. Security ought not to be like linoleum. Linoleum is easy to lay but it is impossible to take up. We have to have security measures that allow us to go up and down with threat levels. Otherwise, we are just going to ratchet ourselves up to higher and higher levels of security and eventually shut ourselves down by creating a kind of neomedieval society.

Conclusions? Security measures include not only deterrent and preventative measures, but all efforts to mitigate casualties, damage, and destruction. We know that deterrents and prevention are difficult to achieve and, therefore, a lot of our attention is going to be focused on response. We know that crisis management and planning are absolutely essential. We know that security should be incorporated into the design and construction of our systems. We know that advance planning is essential. We know that communications are absolutely vital, but communications breakdowns are going to be common, so plan for them.

Those are just some of the brief conclusions. Are there any questions?

JOHN GRIMES, AMTRAK:

Are foreign terrorists more likely, given our border problems?

BRIAN MICHAEL JENKINS:

I am not asserting for one moment that we have so increased security in the United States that we have good control of our frontiers or an ability to control all the people coming into this country. Keep in mind, even from those entering legally, the number of people that enter the country or go back and forth across our borders every year is 600 million. That is more than twice the population of the United States that regularly crosses back and forth across our borders with Mexico, with Canada, into our ports, and into our international airports. Are we absolutely certain that among that population of 600 million there are no bad guys? No, we are not.

What we have seen is, as a consequence of increased intelligence efforts worldwide, that the adversary, particularly al-Qaeda and its affiliated groups, has reduced the number of transactions that make them vulnerable to intercept. For example, they have reduced the number of communications that can be intercepted; they have reduced the number of border crossings, and they have reduced the number of international financial transactions because they know we are looking for all of these things, and these transactions have become more dangerous. I am not saying that they cannot occur. I am simply saying that they have adapted operationally to the new environment by going for higher local content with less connectivity with the top. Like corporations, they are doing a lot more outsourcing and temps in that sense. In other words, they are responding to this in an organizationally sensible way for them. But I have no confidence in the borders; no, absolutely not.

DOROTHY DUGGER, BART:

If I understood you correctly, cost/benefit analysis is not the right analytical tool for the probability of an event, or even a success, but in reality, what we are facing requires prioritization. Are there other metrics in which you have more confidence?

BRIAN MICHAEL JENKINS:

Metrics are a problem; there is no question about it.

I am not saying that cost/benefit analysis should be ignored. When I was on the White House Commission, I learned a fabulous new word from the lawyers on the commission. One of our recommendations was that cost/benefit analysis should not be "dis-positive,"

meaning that it ought not to prevent us from doing something sensible. In fact, I got into an argument with a Congressman in testifying about this. He asked why did we not use cost/benefit analysis when looking at aviation. I said if we applied cost/benefit analysis, we would be looking for ways to reduce the number of safety and security measures because, even if you pile a plane into the ground once a week, flying would still a lot safer than driving private automobiles. We kill 40,000 people a year on the highway in automobiles.

So the question, as we get into cost/benefit analysis, is what are we measuring against? How are we doing this? I am not saying that it should not apply, but I am saying it cannot be the sole criterion for measurement.

In terms of probability, I learned years ago the distinction between analysis and prophecy. One cannot make probabilistic statements. We can make statements about comparative likelihood. I can say that right now, in my view, in this country, we are devoting a tremendous amount of effort to some highly unlikely threats, while ignoring the things that are more likely to occur.

I am not saying we should not prepare for some of these far-fetched scenarios that are now accepted because 9/11 redefined plausibility and no scenario can now be dismissed. But I am saying that we have to think about some comparative likelihood.

We cannot attach a probabilistic estimate to any single event. We can say this event is more likely than this other event, and we can, thereby, begin to rank them. We also can estimate the consequences of each event and begin to use that in the analysis, although I do become concerned about vulnerability analysis becoming a substitute for threat analysis.

This is an important issue because we are so uncertain about the threat. Traditional threat analysis is based on enemies' intentions and capabilities. Since we do not have a good feel for that in dealing with terrorism, we reverse it and instead we start at the other end with the vulnerability, postulate a hypothetical terrorist foe, and outline invariably a worst case scenario. "Suppose terrorists were to…" and insert the most diabolical scheme you can imagine.

That kind of approach is perfectly legitimate for assessing consequences and for addressing preparedness. However, it is not a substitute for a threat. Invariably, what we see is that it is used as a surrogate for a threat. Something that is set out at the top of the page as being a hypothetical possibility becomes probability as you read further through the page. Reading toward the bottom of the page, it is inevitable, and by the time you reach the bottom of the page, it is imminent. We have to be very careful about that kind of process.

How do you deal with security in highly uncertain environments? I think you can do some sensible things and look for collateral benefits. For example, when we are talking about security measures in public transportation systems, we can look at the consequences of deploying additional personnel, or closed-circuit television, or whatever measure we are talking about. While we are not quite certain whether we have a terrorist threat, we do know that the measure will contribute to a reduction in crime on the system, and that is positive. In another sense, we can look at preparedness, our ability to respond. We may energize our ability to respond to consequences or concerns about terrorism, but if that makes us more able to effectively respond to avian flu or Hurricane Katrina that is good too—response is response. You are looking for a set of benefits.

The other one I come back with is to look also for net security benefit. If there is no net security benefit, it is hard to justify the expenditure of public funds for things that are not going to contribute in a major way. That may have to fall in the category of risks we will take as a society. I think we are getting more sophisticated about this and there are ways of addressing this. But to go back to a simple, straightforward cost/benefit analysis, we know that does not work.

FRED GOODINE, WASHINGTON, D.C. METRO:

You talk about cost/benefit analysis and vulnerability assessment and where we should prioritize our funding; then you allude to risk assessment. Can you address criticality assessment? I mean, the vulnerability of a cornfield is that it is highly vulnerable, but how critical is it to our infrastructure?

BRIAN MICHAEL JENKINS:

I think criticality is the key.

In my own ranking of these things, I see vulnerability a little bit differently than criticality. In my own ranking, the threat of immediate loss of life is the number one concern, followed by long-term health issues, social disruption, and economic dislocation. In other words, I want to protect life immediately, then be concerned about long-term health and the kinds of things that can easily lead to social disorder, in terms of huge attacks—loss of control, panic, and so on. That puts economics in last place, although economics are a serious consideration. When talking about the economic effects of 9/11, actual insured costs are going to run somewhere between 50 and 80 billion dollars—a lot

of that is still in litigation. The indirect business-loss costs are high in the hundreds of billions of dollars, probably close to a trillion dollars. That is from an event that cost the terrorists about $400,000 to execute.

SECURITY STRATEGIES FOR MASS TRANSIT

Presentation by Jeanne Lin, Director, Border and Transportation Security Portfolio, Science and Technology Directorate, U.S. Department of Homeland Security

Figure 1 Jeanne Lin

ROD DIRIDON:

Our next presenter is Jeanne Lin, Director of the Border and Transportation Security Portfolio, Science and Technology Directorate of the U.S. Department of Homeland Security. Jeanne was very nice to step in for the Secretary of the Department of Homeland Security, who has been a little distracted recently because of the hurricanes.

JEANNE LIN:

Today I will talk about the Department of Homeland Security (DHS) Science and Technology (S&T) organization, and give you an idea what Science and Technology is

doing and how we are trying to get technology out into the field. Also, I am looking for your input and opinions on developing technology requirements.

Within Science and Technology, two of our largest constituents are border and transportation security, and also the federal, state, and local emergency services. Transportation security is my area, and Dr. Nancy Suski is the portfolio manager for the federal, state, and local emergency services. My emphasis is customs and border security.

When TSA, the Transportation Security Administration, first started, its emphasis was on aviation security. Then there was a realization that rail and transit systems also are very vulnerable because they are so open and accessible.

One of the things that Science and Technology is looking at is technology in the aviation security environment that we can translate to rail and transit; in some cases that may be possible, but not in others because of the different operational environments. First, rail and transit environments are more open, and the throughput is much higher. It is critical to keep that throughput going. We cannot screen everyone, as some of our modeling has shown us. Some risk management must be going on rather than trying to screen every single person.

The DHS approach is to emphasize partnership. There is a growing realization within Homeland Security that we cannot do it alone, so there is more of a drive towards a public/private partnership.

When I was working in the Department of Defense, we had a huge budget compared to what Homeland Security has, so it was a little easier to go off and do our own thing. Our customer base was soldiers, sailors, and marines.

It is different in Homeland Security. While we have TSA inspectors, Customs and Border Patrol, and other areas, we also serve the public sector and so it is not always clear who is our customer base and how we react to that.

The organization chart (page 97) gives you an idea of what the Science and Technology Directorate looks like. Portfolio managers are either threat-based—so they address either chemical/biological, radiation/nuclear, explosives, or some specific area—or they are mission-support portfolios. You may be familiar with some of the existing programs within the Science and Technology Directorate because they are in your transit system area.

Out of the Chemical Portfolio is the "PROTECT" program that the Science and Technology Directorate implemented. It combines commercial off-the-shelf (COTS) chemical detectors along with PTZ, or pan-tilt-zoom, cameras that are networked for a

command center and a local response. The important thing with this COTS equipment—besides the annual maintenance, which appears to very reasonable—is that we are working towards an integrated system, which is very important when looking at overall situational awareness. This program is now with the Office for Domestic Preparedness (ODP), and it is one of the programs that we consider very successful within Science and Technology. We looked at equipment, worked it into an integrated system, and turned it over for transition to users.

We are starting a rail-security pilot for mass transit at the direction of Congress. We are developing a systems architecture in a mass transit environment to figure out how technology can fit in. Do we need to change the process; do we need to work the layout? The threat has been defined as suicide and leave-behind bombers. This is mostly about protecting human life. There is a little about the infrastructure, but more about the number of lives that can be saved and the psychological impact that you are making.

We have done modeling and simulation on Union Station in New York. The New York Metro runs 7 million passengers per weekday. Obviously we have a throughput problem in trying to develop an optimal screening approach. Ideally, you need a system that has low false negatives and low false positives.

As we saw after the London bombings, there are tremendous legal considerations. You cannot do random searches, unlike in an airport environment or in a port of entry where people are coming in and out of the country and it is implied that there will be searches, if necessary. You just cannot do that in a public transportation area. Among the biggest things that we are wrestling with in Homeland Security are the legal considerations.

The rail pilot program is run out of the Explosives Countermeasure Portfolio.

Within our portfolios we lay out short-term and long-term strategies, planning, and how to get things going. We do not have a lot of money, but I have more money than I had in Customs, so I am thrilled with that.

When we conduct studies and analysis, we want to look at things from a systems perspective. When you first start, your instinct is to take a bunch of equipment and throw it out in the field. That may be good for the short term, but, if you are someone wearing a uniform and a belt, there is only so much room around that belt. You are not going to carry things that are not going to support you in some way. If you have a radiation detector that is constantly going off, you are not going to listen to it. You are going to turn it off. If it is heavy, you are not going to wear it. If you have to use something in your hand that weighs

20 pounds, which might be a tremendous stride for someone to develop this technical piece of equipment in the lab, it does not make sense out in the field. So we went from multiple pieces of stand-alone equipment towards integrated systems, looking at situational awareness and a common operating picture.

You want to utilize capabilities where they already exist and insert technology into existing programs. You do not want to create a new one unless you have to, but, if you do, we have that capability. We discovered that we need to work with our customers in a collaborative and cooperative environment and involve everyone. That is one of the reasons why I am here. I am really looking for some input.

One of the things that we have done is to develop a systems model. It reflects not just how technology impacts things but, if there is a policy change or if we modify a process, what is that going to do. In some modeling that we have done for the Border Patrol, we asked if the Border Patrol increases their number of arrests, how is that going to impact jail bed space; how is it going to impact the court system? What are the other implications that you have—both before and after a change—not just on the Border Patrol, or how it impacts Homeland Security, but what about the Department of Justice, and so on?

Our last role is that we want to act as a systems integrator. Within the Science and Technology Directorate portfolio structure, if you have the rad/nuke portfolio that is developing sensors and the explosives portfolio that is also developing sensors, do you want to end up with a system where trucks must drive through six portals trying to get through a port of entry? No, it makes more sense to integrate those and to develop a standardized architecture. Hopefully, it is plug-n-play, with standards that you have to meet in order to put in your sensor.

The approach that we use in developing technology requirements we call a capabilities-based approach. It has bottom-up input from our operators or our users, whom we call "boots on the ground," and it has top-down validation by management. The approach starts with operational workshops to talk about what are the current capabilities and what future capabilities they would like to see. We do a gap analysis. Then we have technology workshops where the technologists get together and discuss what research and development they are doing in this particular area and where the risks are involved. All that information is gathered and we machinate it around and end up with priorities after looking at the gaps and looking at the solutions.

We have done eight operator workshops over the last three years. The first were made up of folks from Border and Transportation Security. We decided that we really had to

concentrate on the Transportation Security side. We realized that it is great to have Border and Transportation Security together and we need to think of it as a family, although now we are no longer part of the same directorate. There were specific pinpoint areas that we needed to concentrate on, so we have had specific workshops for federal air marshals and for aviation security.

This is where you come in. I am looking for input when we do rail security and mass transit workshops. Who should we interview to set up the workshop, and who do you think ought to be attending the workshops? That is your homework.

How do we address capability gaps and prioritization? There are a lot of inputs. It is not just user input; it also is not just all of that stuff that your boss told you that you have to do that is very important. There are public laws and policy guidance that are important.

When we do a technology planning process, we use bottom-up input, top-down validation, and we do gaming scenarios. At the aviation security workshop, we did an "Osama for the day" type of scenario. We had federal screening inspectors, federal air marshals, along with some regulators and some other aviation security folks work together in groups. We gave them broad-based scenarios with some rules and we said, "Okay, you are a terrorist and you have to bring your materials in from overseas; you have to use aviation in some way, so tell us what you might do and how you might do it." Since they had insider information, the exercise was more about where they thought the vulnerabilities are within the airport. A lot of them chose the airport as a scenario because they were most familiar with that. That not only let us know about the vulnerabilities, but also about how technology might help, which led into our actual workshop where we talked about capability gaps.

We have gathered customer input and done a lot of collaboration with the federal air marshals, where communications is a huge issue, and that is being worked very closely with the FAA and TSA. We also do a lot of international collaboration, particularly with our Canadian neighbors, as well as with the United Kingdom and Israel.

Once we get our requirements, they are ranked and rated. In the prioritization, we have the users rank them as high, medium, and low. We then take it to headquarters where we brief the results and recommend where our investment goes.

Some of the areas that the various portfolios within Science and Technology are working on are border related. There is a lot of interest in sensor fusion and multimodal access to multiple databases. How often do local folks hear about what is in our database at the

national level? It is very hard. We ask for a lot of information to get pushed up to the national level, but at the ground level, the tactical level, do we get the information in a timely manner? Probably not. There is not a lot of coordination going on.

Across multiple portfolios we are looking at personal protective equipment (PPE). Nancy Suski, who runs the Emergency Planning and Response Portfolios, is responsible for looking at all PPE.

One area that we are interested in looking at in the rail area is automated scene understanding that looks for leave-behind packages or a change in the picture. We also are looking at different types of cameras for more effective closed-circuit television (CCTV). If you have been in London, you know that they have a lot of cameras all over the place, so we are working closely with the UK to look at their techniques in CCTV, as well as some of the other types of cameras that might be available in other technologies.

I am going to end it there, but I asked you a couple of questions that I am hoping will generate some discussion in this afternoon's sessions.

GREG HULL, APTA:

One of your slides noted the transit connection to critical infrastructures. The fact of the matter is that transit is regarded by the federal government as one of the nation's critical infrastructures and I just wanted to point that out.

One of the issues that we have had from an industry perspective is what we perceive to be a lack of coordination of technology research and development at the federal level. We see efforts being undertaken in various directorates. Obviously DHS S&T, as we understand it, plays the lead role in all of this. We see activities also within the Transportation Security Administration (TSA). In some of the recent outreach that we have had in these various areas, we have expressed our need to understand the roadmap. Secondly, should we be having a roadmap rather than having a better understood coordinated approach to these issues? So, going back to the question you are asking of us—we are going to be setting up a meeting at our association with representatives of the various areas of DHS and TSA so we can begin to discuss what we perceive to be the needs and issues. We have a concern that we have not been engaged in these discussions. We have seen some technologies coming out that DHS is looking for partners to test, and sometimes we say to ourselves, "Where did that idea come from? It certainly did not come from the industry." So, we are indeed looking for that opportunity and we would welcome it.

JEANNE LIN:

You are absolutely right about the coordination. I think both coordination and strategic road mapping are important, but let us work on the coordination first.

STEPHAN PARKER, TRB:

Earlier in your talk, you mentioned random searches not being allowed. Recently, a legal research study was completed looking at the case for search on public transportation, and there are numerous circumstances under which it is allowable. The Transportation Research Board is publishing that. Also, we have a request for proposals out to look for the practical aspects of passenger security inspections.

JEANNE LIN:

That is great; I hope the ACLU agrees with you.

ROD DIRIDON, MTI:

One of the things that we are asked is, what technology should a local transit agency embrace in terms of security screening devices? Every backyard inventor has come up with a sniffer, or X-ray machine, or whatever it happens to be, and it is difficult to see whether or not there is a vetting process established within the DHS or TSA, wherever it is supposed to occur. I think the worst thing in the world would be to have one of the local agencies develop their own system, which is incompatible, and then have to have different training, different parts controlled, and all the rest for every transit agency. Are you making progress in that area?

JEANNE LIN:

I can only speak for what is going within Science and Technology. Within the department, we are trying to do some R&D consolidation. In fact, the Transportation Security Lab, the R&D function of TSA, is coming under the umbrella of Science and Technology. Hopefully, more coordination is going on. Remember, DHS is 22 agencies put together with the hope that now we are one big happy family. But that does not always work really well. As you well know, infrastructure is very important and when we got put together,

there was no infrastructure; there was no process. We are trying to do our everyday job as well as build an infrastructure and a process. I hope we get to that point. I know that among the results that we want to come out of the rail pilot are equipment lists. I know that TSA works on getting lists of equipment out that fall into approval.

GREG HULL, APTA:

The Office of State and Local Government Coordination and Preparedness actually has a clearinghouse for testing technology, and it is available free of charge. Once again, it is one of those things that we came to learn about not too long ago that we need to understand more about as an industry.

IMPLEMENTING THE NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS)

Presentation by Dr. Frances Edwards, National Transportation Security Center

Figure 1 Dr. Frances Edwards

ROD DIRIDON:

I am taking the pleasure of introducing Dr. Frances Edwards because she is our hometown product. Dr. Edwards was identified by the *Wall Street Journal* as the number one emergency response person in the nation, and we are very proud of that. We recently have welcomed her from the City of San José and the region, where she was chair of the regional emergency response committee, into the faculty of San José State University, where she is

in the public administration department and in charge of emergency response education with the Master of Science in Transportation Management program for the Mineta Institute.

DR. FRANCES EDWARDS:

Today I will talk about some of the real challenges that are facing us from the point of view of what the law is now requiring of us. I am sure that many of you, like many of us in local government, are astounded by the amount of new regulations that have come forward with little or no funding support. Given that you have all your other work to do, and now there is a whole group of new compliance requirements, we thought that it might be helpful to run through some of those requirements and explain how we might work together in a collaborative way to make it possible for all of us to find ourselves in compliance for our funding.

As a little background, we know that the tragedy of 9/11 greatly impacted transit. Brian Jenkins and I, working for the Mineta Institute, did an evaluation of transit's impact from 9/11. We found that transit was, in fact, a principal victim, including not only the New York City subways, but also the interstate PATH system.

A little known fact is that there were more transit and transportation workers on site at the World Trade Center (WTC) during the recovery process than any other profession. You heard a lot about police and fire, but all those people in the background, operating the heavy equipment, cutting the steel, helping with welding, were all people from the transit and transportation community. They had been pulled off existing construction projects that were going on in New York City and diverted to help with this incredible problem.

One of the things that most people do not realize is that the plaza where you saw the pile of rubble and all those people working is the roof of a whole series of subway lines. The amount of shoring that had to be done underneath to support the weight of all that heavy equipment and the rubble from the buildings that were never intended to be in one big pile was quite an engineering challenge. The New York City transit folks stepped up, took the challenge, and were very successful.

They also had to deal with the river, which is another thing that you do not hear about much unless you read our book. The wall that protects downtown Manhattan from the river was somewhat compromised in the damage at the WTC. Among the things they had

to do was sandbag the subterranean areas to make sure that the whole downtown did not flood.

So, I want to emphasize the tremendous importance that transit and transportation has in emergency management and emergency response. It is very important that we look at planning from a perspective that ensures those capabilities are there when you need them.

On 9/11, of course, Secretary Mineta, as the head of our national transportation agency, ordered the planes out of the sky. The belief among our security agencies was that was a significant benefit to us in preventing additional carnage, for it appears there may have been other potential suicide bombers in the air.

Bill Medigovich, who was the emergency response manager for the Department of Transportation, tells how he stood by Secretary Mineta and watched what they call the big board that has little colored blips for every airplane in the sky over the United States and in American airspace. That display is normally flashing colors all day and night. He said it was quite an eerie experience to see it go dark, piece by piece, until the only colors left were the military aircraft.

Again, we recognized that the role of transportation and transit is key for our whole country, the way we move ourselves and our economy.

There were some presidential security declarations issued after 9/11 that are now beginning to come home to roost. The first thing the president did through HSPD-1 was to create the Department of Homeland Security to focus on the prevention of terrorism and a response to terrorism. The biggest of the major entities among the 22 agencies were the Federal Emergency Management Agency (FEMA), the Secret Service, and the Coast Guard. In 2005, Secretary Chertoff announced the creation of a Preparedness Directorate and the introduction of a medical officer and the cyber terrorism branch into this already very complex department.

The presidential directive that we are most concerned about today is HSPD-5, which was issued in 2003. It is called "The Management of Domestic Incidents," and has a variety of elements. The ones that are important for us as we talk today mandate a single comprehensive approach to domestic incident management. That did not exist before HSPD-5 because every state had its own method of managing disaster response and planning. The directive also notes that the "Secretary shall develop a national incidence management system," the infamous NIMS, and it says "the National Response Plan using NIMS is the structure for federal support to local incident managers." I must emphasize

this final point that FEMA's role is not as a first responder. The federal government's role is to support local incident managers by coordinating available resources through the emergency support functions. One of those, as you all know, is transportation.

Under HSPD-8, which was issued at the end of 2003, there were some more specific guidelines listed for what was expected of us. The key point here is from the past. If you asked somebody who was a first responder, they would tell you police and fire. If you asked somebody who worked in the field quite a bit, they might have thought of emergency medical services and maybe even transportation in the sense of traffic direction and roads being made available. But under HSPD-8, it is clearly spelled out that the responsibility for protection and preservation of life, property, evidence, and the environment includes public works and other skilled support personnel, such as equipment operators that provide immediate support services during prevention response and recovery operations. Harking back to what I just said about 9/11, you can clearly see that the public works and other skilled support personnel within your agencies—transit and transportation—might be called upon in an emergency.

One more thing, not only looking at 9/11, but also looking at the hurricane events demonstrates clearly that transit and transportation have to be in the forefront of the efforts. Some of the worst problems that developed out of the hurricanes were because of poor coordination within the emergency management structures to ensure that transit and transportation were at the table and able to be effective partners.

Transit systems, as you all know, are victims of many different types of problems—explosive devices and suicide bombers are well-known. We also have always looked to transit equipment as a method for evacuating threatened areas. We have used rail, light rail, buses, and powered transit in many previous events.

We also use buses as temporary shelters extensively in California, and I assume in other parts of the country, because they have the benefit of being able to bring people indoors very quickly; they can either be heated or cooled, depending on the time of year. People have a comfortable seat to sit in if they need to fill out forms, or be given a meal. It is an easy for people to hear what is being announced at the front of the bus, and then they can be given whatever materials they need. We have found in San José that Valley Transit Authority has been a very important partner for us.

Buses have also been used extensively in previous evacuations as transportation for people with disabilities, the elderly, and the poor—people who may not own cars, or be able to operate their own cars, or want to operate their own cars. Buses have also been used as

expedient medical transportation for what we call the walking wounded—people with moderate injuries, but nevertheless who need to be taken for medical screening and evaluation and possibly care. By putting two paramedics on a bus, you can provide a very good level of oversight for people already in transit that allows them to be delivered to an emergency room a little distant from the disaster so that your closest emergency room doctor is saved for the ambulance-driven passengers that are triaged at a higher level of need.

Recovery workers are part of the transit world, as we have mentioned—heavy equipment operators, welders, iron workers, engineers, and people to do damage assessment. But one of the points that was terribly lacking in the Katrina response—and I challenge all of us to try to now build into our response—is that we should not take empty vehicles into the disaster. If we are taking a boat to rescue somebody, we should fill it with bottled water and hand the water out to people that are waiting to be rescued on our way in. We should use our transit vehicles to take in needed equipment as we are bringing out people that are in part of the disaster.

But all of these activities that I have listed here have one common denominator that is hardly ever mentioned in plans, and that is the human element. There is no possibility of doing any of these things unless you have your employees trained and prepared to respond as these suggestions outline—to be the bus driver, to be the heavy equipment operator, to be the welder.

In a picture taken from an airplane you can see that all of those little white streaks are buses; buses marooned in New Orleans because there was nobody to drive them. If you look at the number of them in just one picture, you recognize how many hundreds, maybe thousands, of people could have been saved if there had been a driver for each of those buses. These are 40- or 50-seat vehicles where you could have had people stand in the aisles to meet this kind of tremendous need. They could not be moved, so the buses were drowned and yet there were people who desperately needed their help. New Orleans Mayor Nagin was interviewed about two weeks after the tragedy and he said, "We had plenty of equipment, but we had no drivers."

Let us take that as a challenge to not allow our capabilities to be lost because we did not bring our employees into the planning process early on. And when we talk about our employees, we have to remember to bring in our bargaining units from our various unions. Because in many cases, it is quite a legitimate argument to say that this is not our work. A bus driver is not normally trained or expected to operate in a dangerous environment. They

are expected to operate on normal city streets with traffic control devices operating and the availability of police personnel to respond to a problem. Instead, we are asking people to go into a more dangerous environment. My experience is that when we talked with our represented employees early on and brought them into the process and asked them to be our partners, that we had very successful planning.

I have to give you one more commercial from my side of the world, which is emergency management. Remember, nobody is going to come to work if they are worried about their own family. The only way that you can be sure that your bus drivers are going to be willing to work with you and fill your needs is that they have confidence that their family at home has a preparedness plan, has the supplies they need, has partnered with another family member or neighbor, in case there is a need for help. Then that family member that is your bus driver or your welder or your transit employee is going to be comfortable and confident to stay at work. If they are not, they will go home. In the New Orleans Police Department, experience clearly demonstrates that even the level of sworn responsibility that comes with a badge did not deter people when they were worried about their own families. That is a reality that we need to plan for ahead of time.

The incidents in Moscow, London, and Madrid all show how vulnerable trains can be. There is the long-term victimization of transit in other parts of the world, yet transit can be a partner in solving some of the problems. The security cameras in the London underground helped to identify the bombers.

In prevention, security personnel can be vigilant. It helps to remove trashcans and to change the types of vending machines that are used to make it more difficult to hide devices.

We also are trying to bring the public in as a partner in surveillance, which is very important. The Amtrak campaign poster says, "See something, say something; unattended bags, suspicious activities, a safety hazard. Report it immediately to train or station personnel, Amtrak police, the 800 number, or call 911."

I do not care how many employees you have; you do not have enough employees to be everywhere on your whole system all the time. But there is a rider most of the day in every part of your transit system. Just as we try to bring our neighbors into neighborhood watch type programs to help us with surveillance, this is a great benefit to all of us in transit and transportation to educate our riders about what to look for, to make them our eyes and ears so that we have an extended capability on all of our systems.

HSPD-8 has some very specific impacts on transit. First, a national preparedness goal has been articulated by the president, and it includes some specific national priorities, which happen to be the driving force behind all of your emergency and homeland security planning from hereon out.

These national priorities start with the implementation of NIMS. But they also include expanded regional collaboration. It is not enough for the city to plan, for example, as the City of San José. We now need to reach out to our entire county, to all of the special districts within our county, and to all of our transit partners, which for us includes VTA, ACE, light rail, Caltrain and Amtrak.

You have a requirement to implement the interim National Infrastructure Protection Plan. I hope that all of you have been working with your local law enforcement agency to do the planning that is necessary for critical infrastructure protection, not just the parts of the rail systems that we see everyday, but also the power source. If your system is electrical, where you get your power is a target. If they blow up a substation, the transit agency is not going to be able to run the equipment that runs on electricity, so resources that we are counting on to help us with evacuation can be taken out if the terrorists targeted them. We need to be sure that those elements are included in this planning, so that in the future we can get federal funding to assist in hardening those targets.

Strengthening our information sharing and collaboration capabilities is a very important part of our entire surveillance effort and it requires good coordination with law enforcement, as does strengthening our interoperable communications capabilities. We are pretty good about police and fire now being able to talk with each other through some mechanism. We have also brought in emergency medical services, because we clearly see them in the field.

But we have to remember that transit and transportation are extremely important parts of our need and ability to communicate. If I have a disaster and I need the buses to come, I need a way to talk to the drivers to warn them about any dangers along the route or to give them information about any concerns for passengers. We need a system to do this, and right now, in most major cities, there is no interconnect between transit communications and the emergency operations center, police, and fire.

I was privileged to go to Rockville, Maryland, and visit their outstanding facility where they have integrated their smart transportation center and their emergency operations center. I saw how important it has been for them, even with day-to-day accidents, to have the capability for police and fire, as they respond to a bus accident on the freeway, to be

able to talk to the driver and to have the dispatchers be able to be in communication. The federal government has recognized the importance of that interoperability and has some funding available.

Strengthening chemical/biological and radiation detection response and decontamination capabilities is important. There are great efforts in this with research and development at the federal level.

And finally, strengthen medical, surgical, and mass prophylaxis capabilities. You might say that is a medical issue, but when we think about who is going to get the medical first responders to the place where you want to deliver the prophylaxis, we are going to rely on buses and light rail to help us get our professionals there.

Then, who is going to bring the public? We hope they do not all come in their own car, because there is not enough parking at any of the facilities we want to use. Again, we will be looking at transit and transportation. As your public health department is doing planning for mass medical care, which is clearly in their court, the ability to move around in the community and make mass prophylaxis centers useful and possible really requires a tremendous amount of coordination with transit and transportation.

Another part of the development is something called the National Planning Scenarios. There are fifteen of them. I want to quickly read them to you: improvised nuclear device, aerosol, anthrax, pandemic flu, plague, blister agent, toxic industrial chemical, nerve agent, chlorine tank explosion, major earthquake, major hurricane, radiological dispersal device, improvised explosive device, food contamination, foreign animal disease and cyber.

What's missing?

Flood is the number one disaster in the United States. It is a repetitive disaster that occurs more frequently than any other disaster, and it causes the largest dollar-value losses every year. With Hurricane Katrina, it was orders of magnitude bigger than anything else, and there is no planning scenario on flooding.

My point in bringing that up is that many of the fifteen scenarios they want us to plan for are in the realm of extremely unlikely, such as an improvised nuclear device, or something that is rather difficult for any of us to do much about, like foreign animal disease—that is a Customs issue. Certainly we want to be supporting Customs, but as the City of San José, there is not a thing in the world I can do about foreign animal disease. Yet flooding is a big concern for us.

I think that it is important for us to look at this federal guidance, but customize it to the real world in which we live. When we do our exercises based on the National Planning Scenarios, we need to think of them from an all-hazards perspective. Even if we are focused on a biological event, or a chemical event that is terrorism related, we need to think about how that might support us in other types of events that are more likely.

Finally, the federal government has developed what they consider the 36 target capabilities that are most important. They fall into certain categories. One is called Common Target Capability and that includes interoperability. There are Mission Prevention, Mission Protection, Mission Response, and Mission Recovery.

In Mission Response, I want to point out two things. One is Critical Resource Logistics and Distribution. How is that going to happen?—through the use of transportation assets. The other is a very important piece: Worker Health and Safety.

Drivers not only have to be trained, but if they are going into a dangerous environment, they have to have the appropriate personnel protection equipment, whether it is something as simple as a bulletproof vest or something as complex as a bus that has the right detection equipment. If they must have a HEPA filter or other kind of mask to wear, remember that through OSHA and your state OSHA, every single piece of protective equipment that you give to a person requires training. If you give them a respirator to wear in case they are sent into an area where there is chemical exposure, they have to be trained to use the respirator. They have to have testing to ensure that they are capable of using the respirator and they have to have fit testing for the respirator. Then they have to have training every year. This is not a matter of buying something and sticking it in the bus. This is an ongoing annual cost for training and refresher training.

I think some of these things are lost on some of my Homeland Security colleagues. I go to conferences where they tell me, "Do this." And I ask, "How are we going to pay for that?"

I am sure that your agencies are in the same boat as my city. We do not have enough revenues to just do it. We need to work smarter, because we are already working as hard as we can. We need to try to dovetail activities that we know are important and, as we are doing those, see how we can expand the benefits of those activities into these new worlds that we face.

HSPD-8 says we need to "focus on the capabilities collectively needed to prevent, protect against, respond to, and recover from a terrorist attack or national disaster" and "identify core capabilities" because this is how we "prioritize our federal investments."

Now we come to the heart of the presentation: how you get your money.

Notice that the overarching requirement here is NIMS, the National Incident Management System. Let me read you the quote: "All levels of government across the nation are to have the capability to work effectively and efficiently together using a single comprehensive national approach to domestic incident management."

We can no longer say we do not like incident command systems (ICS) so we are not going to use it. That is the way we now will do business.

NIMS is based on the command and control system called the Incident Command System in the field. This ICS model was created in California in the 1970s. It grew out of the wild-land fires and it is now an internationally accepted method for managing disasters at the field level. In fact, the entire nation of Italy has its entire fire service completely on ICS. Every region has an exact duplication of a cache of equipment so that if they have a big event, they can bring multiple regions together and they all use exactly the same equipment. It is totally interoperable and it is really quite impressive.

There is a NIMS resource management component that includes mutual aid. So, you will need to establish or enhance your mutual aid system.

You need to have emergency operation plans that are constructed along the Incident Command System format, no matter how you had it before, by ESS or your own unique structure. If you want to get federal funding, you are going to have to reformat your plans into the Incident Command System structure.

Jurisdictions receiving federal funds must incorporate NIMS. Beginning on October 1, 2005—this is a federal directive—all recipients of federal preparedness funds must adopt and use NIMS as a condition of receipt of fiscal year 2006 Preparedness Assistance Funding. This does not include just funds from Homeland Security. It includes preparedness funds from all federal departments and agencies. Think about the funding that you receive and the value that it has to you and your agency and recognize that NIMS is now a requirement for you.

On September 8, 2004, the governors received a letter from the president letting them know that NIMS implementation was coming. All of the 2005 federal preparedness assistance programs began addressing NIMS implementation. Transit systems direction for fiscal year 2005—transit system grants are now regional grants—says the following: "Personnel must complete NIMS awareness courses" and "IS-700 is available online."

You must formally adopt NIMS by resolution. It is not enough to just put it in your emergency operation plans that you adopt and run by NIMS and then have your governing board or council adopt the plan. That is not good enough. You need a separate resolution because the federal government wants your governing body to publicly state, "We adopt NIMS and we understand that we have to train on it."

You also have to evaluate your existing compliance, whether you are using ICS now, whether you already have a mutual aid plan and whether it is robust enough. You need to institutionalize both the incident command system and the mutual aid system across your response system.

Fortunately for all of you rail and transit system managers, your city and county partners should already be fairly well along in this process because, like you, their money depends on compliance. But if you work with non public agencies as part of your collaboration, such as utility companies, you need to be sure to bring them to the table so that at least your part of the plan is compliant. You may not be able to get them to comply, but at least the element they work on with you would be compliant.

In order to receive funding in 2006, the 2005 minimal compliance must have been met and applicants are required to certify that they have met those requirements. You cannot just say that you did it. There is actually a certification now that somebody has to sign, which means if you sign it and it is not true, you are in a little trouble with the federal government.

By 2007, complete NIMS compliance is required in order to apply for all grants.

Who needs to take IS-700?

The NIMS Integration Center, which is the national group that is trying to put this information forward, issued a directive in March 2005 that says all personnel with a direct role in preparedness, incident management, or response should take NIMS IS-700 by October 1, 2005, and must have full NIMS compliance within one year from that date.

So who are they? A comprehensive list of people has been spelled out very specifically by the federal government (and listed in my presentation). At the executive level, it is elected officials, anybody that can be charge of anything; it is all of your emergency operations center (EOC) staff; and it is all of your senior emergency managers. At the managerial level, it is agency and organization management between the executive and first line supervisors and all the divisions of your agency that have anything to do with first line response. If you remember ICS, the five boxes are: management, operations, planning

intelligence, logistics, and finance. All of those accountants that are responsible for keeping track of how much money you spent on the disaster have to take IS-700; they are part of the ICS structure at the managerial level.

Finally, all of the emergency response providers and disaster workers, from entry level to managerial level, must take it. Each new bus driver that you hire needs to take IS-700 because that person is the one we were talking about who we want to drive the bus to transport the victims, to transport the doctors and nurses to the mass prophylaxis site, and to bring in the critical supplies.

Who will respond to an emergency in your organization? I tried to make a list: drivers, engineers and conductors, maintenance personnel who are going to have to keep those vehicles on the road, janitorial staff to clean the stations and the cars and who would be part of your surveillance, your ticket agents who are part of that vigilance that we need every day, and then I can only ask you the question, "Who else?"

The national preparedness goals require us to be looking at risk-based targets. This harks back to the first part of the presentation where you need to look at what are your risks, and then what are you going to try to prevent or prepare for, respond to, and recover from—floods, hurricanes, earthquakes, epidemics, the 15 scenarios. The targets are going to be based on your 15 planning scenarios, and I would urge you to include flooding as the sixteenth, whether the feds mandate it or not. Then there is the target capabilities list of 36 activities, which include performance metrics, and the universal task list which has 1,600 items currently and is growing. Somebody in your agency is going to have to look at every element of your emergency response and tie that job to some of those 1,600 universal tasks as part of the evaluation process.

This is when I throw up my hands and say, "Who is going to pay for this?"

This is a lot of information that I have thrown at you. When you go back and try to tell your executive management or your governing body what I just told you, they probably are going to say that I am out of touch with reality. So to help you help them get in touch with reality, I refer you to some websites that are listed in the "Resources" part of my presentation.

If you take the IS-700 course online and you pass it, you will receive an e-mail within a relatively short time—24 to 48 hours. I encourage everybody who takes the IS-700 online to keep that e-mail as their certificate until they get a certificate in the U.S. mail. Forward

the e-mail certificate to your training coordinator and make that the proof document if you get a visit by the feds.

The elements of our national systems are now requiring planning at the NIMS compliance level, operations changes when we have the color codes, equipping for appropriate prevention protection and interoperability of recovery, training, NIMS Incident Command System 100 and 200, Awareness 160 for all your field level people, integration with law, fire, and EMS in your planning, and local specific concerns to be integrated into your training sessions, such as suicide bombing and improvised explosive devices (IED).

Exercises are required. There is a program called the Homeland Security Exercise Evaluation Program (HSEP) that has four volumes of information providing enormous amounts of detail in the kind of exercises that are required: tabletop, facilitated, and full-scale exercises that bring together your first responders to have them practice.

How can the Mineta Transportation Institute help you?

We are here today not just to scare you but also to give you some encouragement. A tremendous amount of research has been done that is available at http://transweb.sjsu.edu, the MTI website. We also have other materials available that we hope will be helpful. We offer guidance in plan writing if you are concerned whether your plans are ICS compliant. We can help you with planning assistance on how you are going to comply with the national response plan. MTI can provide assistance on the preparation of federally required documents, including answers to your questions about who needs training in what courses.

I want to spend my last few minutes talking about exercises because exercise programs are really the key to preparedness. You can write a great plan, but if nobody knows what is in it and nobody has ever tried to use it, all you have is a really nice doorstop. What you need is a plan that is embedded in people's heads.

The excuse in New Orleans for why they did not do a better job responding was, and this is a quote from Mayor Nagin, "My plan was in the trunk of my car, underwater."

That is not an acceptable excuse. Your plan does need to be in the trunk of your car, arguably, and it also needs to be at home in a safe spot, but most important of all, it needs to be in your head. I am not suggesting that all of you are going to memorize your whole plan because you are not responsible to do every job in your plan. The only way you are going to embed your job in your head is to do it in an exercise environment, not once, but annually or more often if you have the capability.

Exercises are really the key to your preparedness. All the rest is prologue. You can plan. You can write a nice document. You can buy the equipment. You can train your personnel in all of the skill sets. But if you never practice, when the time comes to do it, people are not going to instinctively do what the plan says. They are going to just make it up as they go along, and therein is disaster.

We urge you to look to MTI for any assistance that we can provide. This may be with tabletop exercises for your executive management so that they understand your goals and their roles in a disaster. It may be with drills for your field level personnel to ensure that they have the skills that you want them to include.

I urge you to do an annual drill of family preparedness. It does not cost much money. You can partner with your local city or with your American Red Cross chapter. The Red Cross has wonderful handouts and people that will do one-hour lunchtime brown bag presentations on how be prepared at home. It is an excellent investment, both in your employees and in your organization.

The Mineta Transportation Institute can assist you with a program called Facilitated Exercise for First Responders. The Harvard University Kennedy School of Government has selected this program as a best practice. They have written a case for their executive program on crisis management that was funded by the CDC. We have several partners who have certified or agreed that this is a really good way to do exercises.

Recently, I had the thrill of being part of the first facilitated exercise in my jurisdiction that involved our rail partners. We went to the Union Pacific rail yard, where ACE, Amtrak, and Caltrain brought equipment and let us use it for three consecutive days of classes. We put almost 300 first responders through the facilitated exercise. They learned about improvised explosive devices and where they might be hidden in rail, light rail, and buses.

They were given an introduction to railcars, because most police and firefighters have never been close to a train or ridden a train. In California, trains are not part of the day-to-day life of most people. If they have to respond to your equipment, they need to know what is safe. Where are the high pressure hose lines? Where are the fuels? How do they shut them off safely? Where are the hazardous materials? Where are the human waste containers for the restrooms? They need to know so that when they try to provide assistance they can be safe, and they can make your passengers as safe as possible as they extricate them safely.

One thing they did not know is that railcars today are built with unibody construction. Their first thought was to take the jaws-of-life to it. But what happens is the car crumbles likes a beer can. What they learned was where the decal on the roof is that shows where they can safely cut to get the victims out if the train has derailed on its side. Where are the locations of the switches to open doors? Now they know where they are. We gave them full color handouts to put in every rig, not only for the City of San José and the County of Santa Clara, but for the entire ACE train rail line as well.

How did we do that? We did it with the Homeland Security funding that came to ACE through the Urban Area Security Initiative (UASI). Look to the availability of money that you have now and see how you can make it go farther. ACE paid $96,000 for overtime support and the City of San José Metropolitan Medical Task Force provided the instructors, the handout materials, and the learning opportunities.

This was a tremendous joint venture that we were able to accomplish, and it is something that you can do in your jurisdiction. It does not have to be difficult. It does not have to be expensive and it can be incredibly productive for you and all your partners. Then, when you are ready, you can do a functional exercise in your emergency operation center or a full scale exercise in the field. The facilitated exercise will embed the plan in the minds of the people who come out and learn and do together so that when a real disaster occurs, they are a team, coordinated, working together with our federal partners under NIMS to succeed for the most important reason possible, to save the lives of people in our community.

ROD DIRIDON:

Dr. Edwards has described the capabilities within The Mineta Transportation Institute. There also are commercial organizations that provide similar kinds of training programs.

If you are not complying with the law, you ought to be, and not only for the sake of protecting your people. If you do not comply with NIMS, there is not just the danger of your constituency being killed or your economy being disabled for an extended period of time, or maybe permanently, but also there is legal liability.

This is the law. In California, it has been the law for a long time with SEMS (the Standardized Emergency Management System). If you have a disaster in your local community, and it is determined that you did not comply with NIMS, those who are hurt by the disaster who might not have been hurt if you had been properly trained, have a legal

cause of action certainly against your jurisdictions, but possibly against you as individual managers of those jurisdictions.

Those are the facts of life, yet we are so busy at the local level that most of us do not even know what NIMS is. You are the best of the crop, because you took the time to be here. Your counterparts out in the community, who have just as much concern, should have had the training by now to be completely compliant. We have to take this to heart, not just because it is the right thing to do, not just because to do it saves lives and gets you back into business quickly, but also because of the legal liability.

Do you have any questions?

JAMES RUDY, ORANGE COUNTY TRANSPORTATION AUTHORITY:

We have taken the online course and apparently we have heard from the State of California that they are not going to recognize that, or at least POST (Peace Officers Standards and Training) wants to mandate training for first responders. Have you heard any update on that?

FRANCES EDWARDS:

Yes. We have our own overlay in California. POST has a course that is mandated for all sworn law enforcement officers and it has elements of AWR 160 in it, but not NIMS. So you have to do both the NIMS IS-700 training and the POST course. Through the POST course you will get compliance with AWR 160, which is the other course that officers and responders at the field level must have. Suzanne Mencer, who was the head of the Office of Domestic Preparedness in 2003, told us that AWR 160 was a priority, so that is what we have been doing. When that grant came out, most of us put our emphasis on AWR 160, because we were told if you did not have that done by 2004, we would not get any more money. Now NIMS has slipped in as well. Also in California is a course that the fire department has to take which includes part of the AWR 160 requirement. So in addition to NIMS, there is AWR 160 for all of your field-level people.

KATRINA KERNODLE, FRANCES KERNODLE ASSOCIATES:

You showed the picture of the "See something. Say something" Amtrak messages incorporating the many riders on the transit system into the security campaign. I also wanted to mention Transit Watch, which is the FTA/TSA initiative that was launched at the APTA meeting in 2003. I know San José was one of the first cities to be a Transit Watch community. We are doing another Transit Watch initiative right now, and if you want some informed answers, you might want to speak with Bridgette Zamperini with TSA. She has a lot of information on Transit Watch.

FRANCES EDWARDS:

Since we are in Dallas, I should mention that the local mass transit company here also has a very active campaign and they produce a newsletter for all of their riders as well.

MARK OSTERTAG, CAPITAL METRO, AUSTIN:

One thing that you mentioned surprised me. Having all of our emergency management team and all those responders be IS-700 certified is not an issue. But it causes me concern when I am dealing with my operators and maintenance people. I bring them in quarterly for training. In the last 18 months, which would have been six sessions, one-half of the sessions were on emergency management. We have had NIMS since I got there and we regularly do field exercises with the city, as well as tabletop exercises and all the things you are saying we should do.

But now must I also bring in all of these operators and have them IS-700 certified as well? Must I come back a fourth time in 21 months to do that?

FRANCES EDWARDS:

The responder level is any emergency response provider and disaster worker, from entry level to management level. This includes public works/utilities and other emergency management response personnel.

You could talk with your attorney to see whether he feels if that is a correct definition. The attorneys that I have spoken with that are dealing with mass transit in California are advising that anybody that you are going to send into a disaster needs to have IS-700

certification. If you have somebody that you are going to ask to drive a bus for evacuation or transport of critical personnel, they would fall into this rubric.

On the Internet, there is a document from the State of Iowa Department of Homeland Security called *IS-700, Who Needs to Take It?* That could be something your attorney could review.

I took the three quotes from the Department of Homeland Security document http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf.

There is also an information bulletin from the Department of Homeland Security that addresses NIMS compliance, and there is a NIMS section on the FEMA website (http://www.fema.gov/nims/index.shtm). Listed there are many resources from the NIMS Integration Center, including the fact sheet: "IS-700 and ICS 100 and 200: Who should take them?"

Actually, there is a tremendous amount of documentation about NIMS.

RICK DUCHAME, TORONTO TRANSIT COMMISSION:

When comments were been made about passengers sighting articles that might be lost in the system and using that as a community-wide type of thing, I cringed. That is a very serious issue with us in Canada. Although our transit system does not have the ridership that New York does, we are the third largest in North America. To put it in perspective, we carry 1.4 million passengers a day; we have 30,000 lost articles a year. Suitcases and knapsacks? We get five a day. We cannot have our customers be the eyes and ears because, as Brian Jenkins mentioned, you better not do it unless you can respond.

Be very careful when you make presentations to bureaucrats and politicians, because it can be very dangerous for system operators like us. I know in Canada, when talking to our own federal ministers, I must be careful of them thinking we can do that, because we cannot respond. I do not think something that is one solution that fits all. That would be my only caution.

BRIDGETTE ZAMPERINI, TRANSPORTATION SECURITY ADMINISTRATION:

We have worked in cooperation with the Federal Transit Administration, and the Kernodle Company as well, to promote public awareness. We developed the "Transit Watch"

campaign. One of the things that we did, in talking with state transit corridor personnel, is to provide a general template for the agencies to use if they would like to use it. That allows them to consider their needs and the size of their systems and develop materials that are going to work best for them. That is something we definitely encourage because we realize the parameters of transit agencies are different across the board. So, we are not talking about a campaign that is the same across the United States. They are definitely used differently, and we respect those differences.

MIKE SETZER, SOUTHERN OHIO RAPID TRANSIT AUTHORITY:

You said something about the unfunded mandates. I do not expect you to solve this for me, but on behalf of the transit agencies that ultimately will have to carry all of this out, I just want to express the concern that, especially in middle-sized cities, the threat of these kind of cataclysmic disasters exists, but the reality is that we are challenged every day, right now, by ordinary street crime. A high school student was shot on one of our buses last week. My concern is that the very resources that would be redirected to this kind of national preparedness, whether it is operator training or emergency center personnel, those are the resources that are already meager that are being applied to keeping our passengers safe from things that are not threats, but are, unfortunately, recurrent realities. Ultimately, either we are going to have to get some more funding to do this, or we are going to offer our passengers less service. I think that is a poor substitute and I suspect other people in the room feel much the same way. I understand that you cannot fix this, but I do not want to dismiss it that easily as another unfunded mandate.

FRANCES EDWARDS:

First of all, I feel your pain. I am in a city of 925,000 people. We have 1,700 police, 800 fire fighters, and numerous public works people. We cannot figure out what constitutes 100 percent compliance, and we cannot get the feds to tell us either. I asked, "If these are your rubrics, who are you talking about when you say medical care or transportation?" The first problem is how do we get a better definition of what is really their bottom-line thought?

There are Homeland Security grant funds that go to every state in the United States and are supposed to be threat based. In the larger cities, like Cincinnati and Cleveland, there are also Urban Area Security Initiatives programs, so transit agencies should look to one of

those sources of funding support for their training. What we have done in San Jose is a city-sponsored, train-the-trainer opportunity for AWR 160, for example. The Valley Transportation Authority provided the facility for us and we provided all of the other costs. The feds gave us the instructors for free. Now we have 93 people trained that can go to any agency that needs help. I have three policemen that are trained, but they can train transit workers because the information is the same.

IS-700 training is web based, so one strategy is to get all of the office people trained first because that is essentially no cost. You are diverting two to three hours of their time, there is no doubt about that, but when they are sitting there, they can still answer the phone and if an emergency happened they could still respond to it and then come back to the training project later.

Other things that some agencies have done are to either give people compensatory time for training at home over the weekend, or to give people overtime if they are under bargaining-unit representation.

There is no easy answer. I would suggest that you talk to both your state Homeland Security grant folks and your UASI folks because there may be some way to do a regional project that would cut down some of the costs for everybody.

Since we have APTA here, I want to say that until we make it clear to Congress that just telling us to do something does not accomplish anything, we are going to keep getting told to do things. To whatever degree you have lobbyists or professional organizations who can try to make some of these concerns clear to the Congress, the better.

What Congress has done is eliminate the UASIs that were given to each of the major transit agencies last year, and instead created this combined transit grant. In the San Francisco Bay Area, we have had numerous meetings over putting together the proposal for the transit grant. When the money comes in, it seems to me that there is going to be a fight over who ends up actually getting it. One of the priorities for the transit grant funding, at least the first year, ought to be to get everybody NIMS compliant so that you can go forward.

There is a real temptation to go get the toy catalog and to buy toys [equipment], but the most important thing you can do is train your staff. The toys can come later; if the people are not trained, the toys do not matter.

BUSINESS CONTINUITY MANAGEMENT

Presentation by Mortimer L. Downey, Chairman, PB Consult, Inc.

Figure 1 Mortimer L. Downey

ROD DIRIDON:

How we get back to business is the toughest part of this formula. As much as we are concerned about the threat and security and emergency response, getting back to business in the United States is tough.

The Londoners showed us how to do it when they had their bombings. The next day, they were all back on the subways going to work. We are not as used to it as the British, as a result of all the sensitivity that they acquired through the IRA experience.

We tend to overreact. Remember that a real target of the terrorists is not just to kill people, it is also to kill our economy. If we do not get back to work, they win.

Please give your attention now to Mort Downey and his panel as we discuss procedures for getting back to business and maintaining the preeminence of the North American economy in the world marketplace. Mr. Downey is a world recognized researcher, academician, public administrator, and now a corporate leader as the new chair of the Parsons Brinkerhoff company PB Consult.

MORT DOWNEY:

I want talk about the issue in the context of calling it business continuity management, and I will explain that in a minute.

Considering the recent security and disaster issues, this is a very timely conference—whether we think about the aftermath of the gulf coast hurricanes, the London bombings, the Amtrak derailment, or the anniversary of September 11 falling within the last few weeks.

As we think about all these events, they remind us that as we plan we have to keep in mind all hazards. We also have to keep in mind that the timing of these kinds of events is almost never anything within our control. Then we have to remember that a plan that is on paper (or maybe in the trunk of the car), is no assurance that we have a strong ability to deliver when events occur. That is what business continuity management is about to me.

Today we have talked a lot about responding to an immediate event. But in fact, those of us who are managing businesses, managing transit agencies, or managing the economy have to be able to respond effectively and over a continuous period. It seems to me that if we cannot provide business continuity management, we could be in the position of saying "the operation was a success, but the patient died." We have to be able to keep business going, maybe not business as usual, but possibly business as unusual. It is not simply a process of recovery from disaster; it is a process of managing your business in such a way — that you are resilient, that you are able to deal with it.

There are principles that we are going to talk about. Today I am putting them in the context of transportation agencies, but in fact, they are universal for businesses or even the economy at large.

Before we began this session, we were chatting about how transportation affects things. Steve Flynn, who has written books on the subject and is frequently seen in public hearings or on television, posits the idea that if we do not have solid control of how the economy and the system works on good days, we will fall apart on bad days. For example, if a container crossing the border holds a nuclear device and it explodes, it clearly causes a local issue of significant concern. Unless we plan for it, his fear, and mine, is that the response will be shutting down the entire freight system in the country until we have inspected and certified every container that was in motion.

If you remember the shutdown of the West Coast ports in 2002 by a management lockout, the ripple effect of that was enormous across the entire world. It brought assembly lines to a halt and it caused billions of dollars of damage, all from a known event that there were ways around.

If we shut the entire system down to inspect today's 20,000 containers, which will take us about 42 days to do, there are another 20,000 coming in for every day thereafter. How long would it take us to get out of that? At a smaller level, if your transit system is shut down and has to rebuild and reopen, what does that mean to the community? We really have to have a mindset about business continuity management, or else the economic damage, the collateral damage of the terrorist act or any other act, would be a disaster to our economy.

I remember when I was in DOT, and we would sit down with our friends at FEMA before events, not during them, to talk about how did we prepare. What do we put in place? How do we respond? They would always remind me that transportation is ES-1, Emergency Service 1. Nothing else with regard to a response works if you cannot get people to it, people away from it, goods there, and support for first responders. ES-1: that is how significant transportation is in managing disasters. That is also how significant it is in making our economy work.

Brian Jenkins talked about the difficulty of analyzing how much we should spend or where we should spend it and correctly said that we have to make some intuitive judgments. We have to do things that we think will be beneficial, and hopefully beneficial in more than just a response point of view, but actually have positive benefit. I have been espousing this for some time on the basis of little or no evidence but as clearly a good idea.

Fortunately, someone has come along and written a book to provide that evidence. It is called *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*, by Professor Yossi Sheffi at MIT, who is a noted scholar in transportation and logistics. He is making the point that the business entity that can respond resiliently to a variety of unexpected

circumstances is not only protecting itself it is creating a competitive advantage. The ability, under those circumstances, to provide appropriate service before, during and after a calamitous event is an important element in managing a business. Sheffi shows in his book how company fortunes in the face of business shocks, whether natural or manmade, depend more on the choices made before the disruption than they do on actions taken in the midst of it. The measures taken to invest in resilience really are creating competitive advantage and giving you a better capability to run your business.

Another British study looked at organizations that had thought about and created a process to respond to crisis versus those that had not. They came up with the opposite negative finding that reinforces Sheffi's positive finding. An organization that has not thought about crisis is seven times more likely to think that it will not have any impact on them. I do not think they are right.

These are the same issues that confront our transportation system managers. The likelihood is high for all of you who have been in the business for a number of years to recognize that every manager is going to confront crisis at some point in his or her career, whether from a natural disaster, technological failure, or intentional disruption by terrorists or others. It is going to hit you. One thing to keep in mind, in addition to the legal liability issue, is that the manager's performance under those stress conditions brought on by crisis is going to be the basis on which his or her performance is evaluated for many years after the event. Those who do well will be remembered for it and rewarded for it. Those who fail that stress test are going to have that mental picture in the public's mind for a very long time.

Building the issue of resilience into your organization is something that we need to think about; that is a term that you hear in Dr. Sheffi's book. We have some thinking going on about this in London, where I do a lot of work with the transport system. They are about to issue their new five-year capital plan and a lot of money now is being diverted into preparation and resilience. Those investments are not just something that will sit on the shelf until the next time there is a bomb. This is going to be investment in better communications, better capability in their signal systems, and better ways to communicate to the public. These upgrades will be used every day and they will make it a better system every day. But they particularly will make it a better system in terms of response.

The key for business continuity management is not just that it is a job for the senior manager. I would argue that it is an issue for the entire organization. The ability to work through the plans, to execute the steps that will be part of business continuity is really a

function of how well managers understand their business and how well they actually manage in doing it.

Finding and securing the factors that are necessary to run your business is not just what makes it perform well in crisis, it is a key part of everyday success. It is not just what you do after the event occurs; it really runs through the entire cycle. Business continuity is something you need to be thinking about when you are focused on an emergency—the preparation for it or the ability to mitigate it. Business continuity certainly is part of response. When you are out there wrestling with the alligators, you still have to be thinking about what business you are in, and how you are going to do it well.

Business continuity is critical to the issue of recovery. We talk about who is responsible for recovery, but I think the clear picture is, for those of us who are in the transportation business, we are the ones who really are going to have to take accountability for recovery and for making sure that the patient does live.

If you look at the national response plan, in terms of priority, you find that facilitating recovery ranks seventh and last in the priorities within that plan. I would argue that is probably correct when you think about saving lives, protecting homeland security, supporting law enforcement, or protecting property; those are probably correctly ranked above facilitating recovery. But those are the things that the emergency responders and the NIMS structure will be dealing with. Thinking about what comes after is our headache and something that we need to be prepared for.

When I was in the Department of Transportation, the Coast Guard was part of DOT. They are still a high performing agency in Homeland Security and we certainly have seen what they can do during Hurricane Katrina. A television morning show today was interviewing a couple of helicopter pilots and making the point that Coast Guard helicopters saved 33,000 people and flew thousands of sorties. A young woman pilot talked about bringing ten infant children up into the helicopter and getting them away from a flood site.

The Coast Guard is always ready to do what they need to do. In fact, the Coast Guard motto is *Semper Paratus*, Always Prepared. They backed it up with something else when they were talking to me, because I am an old Coastie. They say, "Proper planning prevents poor performance." That is their watchword: getting prepared, thinking it through, having a program in place, and ultimately executing it well.

I do not how many of you had this experience, but when the after-action reports are put together it is very seldom that the performance in the event exceeds the expectations of the plan. At best, you want to meet them or come close to them. But if you have not done the planning, you will come nowhere near those expectations.

What are some of the key elements that are part of a process of developing a successful capability for business continuity management? I talk about it as developing capability, not checking the boxes on a checklist, but really thinking it through and living it.

We will talk about some real life examples in our discussion this afternoon. The successful cases do have some key factors in common. I would argue that the planning process has to start from the top down. It is senior management's responsibility both for outcomes and for results. I am sure we will hear that successful plans are the ones that have been tested and honed through training, through exercise, and through continuous approaches to making them work.

I think the organization that is resilient, that can respond and continue its business, is one where that whole activity has become part of the culture of the organization. Again, it is not something that just resides in one part of the organization. I know there are a lot of people here today whose responsibility is security, but you are not off the hook. You have to tell your senior leadership, the people up the line in the organization, what their responsibilities are and how those relate to what you are doing.

Ultimately, we have to recognize successes. Successful efforts deserve recognition if we want to build that into the culture. Again, going back to my DOT days, we would have an annual awards ceremony in a very prestigious large hall in Washington. Hundreds of people would be there and the poignant elements of that was always the recognition of honors of people who had responded well. It was not just the helicopter pilot who bravely rescued people 200 miles out to sea, although we had lots of those, but also others. Any time there had been some event of great significance, whether it was the Mississippi River floods, or the aftermath of aviation disasters, we always recognized the team who had been part of that, and said, "That was an important performance; that was above and beyond what we expect."

Not surprisingly, as we are looking to make sure that the patient survives, the things that are important in business continuity look a lot like what you need to do on a day-to-day basis. Success in the stress-test environment requires the same tools and the same factors. You have to think about how to make them available and how to be sure that you can have access to them. Thinking about continuity means thinking about personnel, supplies, your

maintenance capabilities, about information technology, public affairs capability, communications capability, and thinking about finance. You would not open your doors on any given day without having a good handle on these issues. One day you may have to open your doors and find something outside that you do not like, and you will need an even stronger grip on these issues.

There are some other things that perhaps you do not think about in a normal day, but certainly you need to be prepared for. If someone has put a chemical or biological attack in motion on your transport system, you are moving into uncharted territory. How do you clean up from that event? Who will tell you when clean is clean enough?

Thinking about how you might respond is a useful and important exercise, because you will be at the forefront of not only responding, but, more importantly in terms of restoring the public's confidence as the system returns, people are going to want to know from you that it is safe and they can come back. You have to think through how you will do that.

Other things outside the normal are things like staging emergency evacuations, restoring service to damaged areas, and operating under the constraints of a law enforcement declared crime scene. If this is a suspected terrorist event, all of a sudden you are going to have lots of partners in what is going on, and they are not going to want you to restore the system until you have dealt with every piece of evidence they can collect. That will be a time of great tension. It would be helpful if you have talked with law enforcement ahead of time about what that means and perhaps reach some accommodation of how soon you get back into business.

There are a lot of things that need to be included in the planning effort. You need to look at risk assessment. Where should I really concentrate my efforts? What are the kinds of disasters and events that most need to be dealt with in terms of business continuity? If floods are going to happen frequently, it might make good sense to have a business continuity plan to deal with that. Other events may be less likely to occur, but if they are incredibly severe in terms of what impact they might have, they also deserve thought. In terms of thinking about those risks, it is probably beneficial to think about some worst case scenario. If you are prepared to at least contemplate what you would do under those circumstances, any lesser response is going to be that much easier.

Most importantly, you have to think about understanding your business. What would you need in order to open on a normal day? What would you need under emergency circumstances? And who knows that better than your own managers? They are going to be

accountable for undertaking the business in these circumstances. Get them involved in preparing the plan and then hold them accountable.

Another key factor is building relationships. When you are trying to get your system back in place after an incident, there will be no time to suddenly try to figure out who are your suppliers, who are the other entities that are involved, or what other responder groups are out there working. You need to have developed those relationships already, and that happens through the process of training.

You need good relationships and understanding with your union representatives. They are part of the process. They are part of the leadership in identifying what your employees will do, and building a culture that, under unusual circumstances, we ask for unusual responses.

You need trusted relationships with the senior government officials who are going to be making decisions, either with or without your input, so at least they will talk to you about what can and cannot be done, about what is realistic, and what you can expect.

You need to have good relationships with your counterparts in transportation agencies around the region and around the nation. Reaching out for help, particularly if this is a localized problem, is something we should all be ready to do. I would argue that it is something we should be thinking about and making plans for every day.

Finally, in terms of thinking ahead, you need to establish clear priorities for everyone. Certainly the first priority has to be safety, the protection of life. You cannot take extraordinary risks only to say that you may have killed a few people but you got the electric power restored so the trains could run. We have to think about safety. We also have to think about steps that might be taken that potentially could make the situation worse, and then avoid those. Take steps that avoid cascading problems. Get to the physical integrity of the system and then ultimately to management and administrative requirements. But the first priority has to be safety and the preservation of life.

What are the things that need to be in a plan? If you look for the elements of a successful plan, what would you be looking for?

First, it has to be simple and understandable. It has to be well distributed, out in the hands of people who will use it. It has to be updated frequently. As you bring new facilities, new services, and new procedures into place, you have to fit those into the recovery plan. For instance, how about the new maintenance facility; how does that fit in?

It has to be one that people live through the drills, the exercises, and the efforts to embed it into the culture.

It needs to be clear in terms of assigned responsibilities. The memory of Al Haig coming into the White House press room saying, "I am in charge here," is not what we want to do. We want clarity as to who is responsible, what it is they are assigned to do, and who their backups are. If the person that is responsible for a particular activity may become disabled or unable to reach the scene, the chains of command have to be clear. Everyone involved needs to understand who is in charge, where they will be located, and how people will communicate with them, with no freelancing.

We have to think about what are the key facilities. Where will emergency operations centers be located and are the equipment and supplies needed for a good EOC in place? Other key facilities in the system need to be thought through, like maintenance shops. Do we have enough capacity? What if we lose some elements of a facility, how do we restore operations? Are there backups? We know of some major transportation systems where all control is operated out of a single point and there is no backup. This is not a good idea.

A particular example might be the Washington Metro looking for support from the federal government to build a secondary control facility. Because more than half of the federal employees in the District of Columbia metropolitan region come to work and go home on Metro, we cannot have that entire system brought down by pinpoint failure in a single control room if there is an evacuation. Thinking through what exists, what we need to do to protect mission-critical facilities and mission-critical services, and what we have as backups must be part of the plan.

Another key part of the plan, obviously, is people. How do we contact them or issue instructions to them? Do they understand their responsibilities? What are they to do if they are not communicated with through a breakdown of the telephone system or otherwise? If you cannot communicate with them, they still should know what to do in that situation. You also have to know that you can contact the right people. That seems pretty simple, but how many of us have experienced that failure? "I thought I was on that list; or, who has a list of where people live, their phone numbers, and how to get a hold of them?"

I recall years ago when I worked for a transit system, one of my responsibilities was to be told when there were serious events. Well, I left and went to Washington, but my family was still in the New York area. My wife did not mind getting these calls. But when we would go out on a Saturday night and the babysitter would get a call saying that a person

has been killed by a train in Jersey City, she would get very nervous about that. Obviously, the person who needed to know this was not hearing it because the list had not been updated. I learned that lesson, and on the day I left DOT in 2001. The last call I made was to the operations center, saying, "Take me off the list; I do not need any of those calls from the middle of the night. Here is the name of my replacement; call him."

When thinking about staff and job assignments, you need to include cross-training. Consider the critical functions that need to be performed—whether they are management, operational, administrative—and identify a number of different people all of whom have the ability to perform those functions. Everyone will be under stress and some people may not be at their jobs. But if it is a critical job, we have to be sure that there is somebody who is going to do it. Family preparedness is another key issue that is part of getting people to be willing to put their time into the recovery program, because they know that their families are being taken care of.

There also is the sensitive issue that a certain number of people are not essential, but you do not want to tell them they are non-essential. In these cases you need to have a staged response. For the first week or so, ask them to call in and let you know that they are alive and available to work when needed. We do not want to happen what I remember seeing when I was coaching soccer for six-year-olds—the point when the ball is going one way and all eleven people on the field run towards it. We need an orderly process and that means we do not have anybody there until they are really needed.

Information technology certainly needs to be part of a recovery plan, maybe even more than others. We know that IT facilities, on the best of days, are subject to all kinds of problems. If they are not backed up, you are in trouble constantly. In fact, it might be that the cause of your emergency comes about because of an IT failure, whether it is the typical programming problem or whether it might be a cyber terrorism issue.

I worry about the openness of the control systems in many of our operations. I am afraid that any self-respecting hacker could get in there and bring the system to a halt. What do you do if that happens? If you are in a major recovery mode, certainly you are going to need IT and you are going to need it early. I hope that you can say that you have offsite facilities and data storage elsewhere. If you do not, you are certainly running more of a risk than you should.

Similarly, when you get into a recovery mode, you are going to need access to your records, whether they are financial, engineering, employment, or inventory records. Will you be

able to get them when you need them? Have you thought through what you would do if you did not have access to them? Take the appropriate steps.

I was in Japan shortly after the Kobe earthquake. One of their headaches was that all of the engineering records for public facilities and services were in one somewhat earthquake-prone building. They were on the fourth floor, which, by the time the earthquake was over, was also the third floor and the fifth floor because everything pancaked down. There was no way to get at the records. It is very hard to rebuild if you have no access to your records, so think that through.

Also, record keeping during execution of the plan is important. Somebody has to be assigned to maintaining a log of what has happened. You know that there will be follow-on reports and discussions of who did what when. You will need to know the costs. Ultimately the opportunity for reimbursement will exist, but only to the extent that records are available. Records are a part of every day business and they have to be part of business continuity management.

Insurance may be a potential issue. You need to look at whether there is insurance coverage for any of the things that have occurred. If not, you need to see if you can get coverage, although it is harder and harder to get coverage for any of these issues.

Finance certainly has to be part of the recovery cycle. Nobody ever has enough money in their budget to cover the costs of every emergency. You would have a terribly fat budget if that were the case, and people would come after it. But prudent planning has to question how you assure continued operations when there may be no revenue coming in and an extraordinary amount of money going out.

While ultimately you may be able to recover, or get support, you are going to need that money day in and day out during the recovery period. So, where will you go to get it? Is it to your own internal contingency funds; is it to your sponsoring agencies? I used to say when I was at MTA in New York that the last step is the rail ticket up to Albany. As long as we could pay for that we could at least go ask the state legislature for some support. Your financing may be from external sources; you may need a line of credit from a bank. You really need to think through what will keep your payroll going and your costs of immediate supplies paid for in that situation.

Communications are a critical part of the plan. Consider how you will notify the public of what is going on, the current status of the system, and the steps that they should be taking. Determine who will be the spokesperson for the agency and how to assure that that

person is someone in whom the public will have utmost confidence. Panic will spread if information is not clear and if the spokesperson is not believed. When I was on the National Academy of Science Task Force on Terrorism Response, we talked about scientific response. We thought that one good scientific response would be the ability to clone Walter Cronkite because that is the type of person you need to have.

The spokesperson has to really know what is going on. How do you collect information in such a way and get it there correctly to someone who can deliver it? This need is going to continue well beyond the response phase; it is going to continue into the recovery phase. As system operations are gradually restored and as hazardous conditions are eliminated, we have to get that word out. The goal is to be sure the patient recovers, that people come back to the system and that riders return. This only happens if the public regains confidence.

Some interesting research was done a couple of years ago based on Tel Aviv experiences, and is now being applied in London, on how long it takes to recover your ridership after an incident. It turns out that people who have to use the system grumble a little bit at first, but once they have crossed the threshold that they cannot get to work without using the system (and they survive the first day), they are back. But the people who have a choice will take months, if not years, to overcome their fear reaction to not go there. You have to be able to ease them over that threshold, or else you will suffer a long-term loss.

Another part of a successful plan is support agreements. Where will you get the operational factors you need? Do you have contracts in place that cover continuity services that you will need for fuel, equipment, maintenance, or clean-up? Some of those arrangements may become overtaken by events. In a disaster of major consequences, ultimately it probably will be the federal and state officials that are going to start parceling out what is available. But you need to know, even in those circumstances, what your needs are and how much of certain commodities you need to operate your system.

Lastly, and it should be both first and last because nothing is more important in a business continuity plan, is that there be a robust program for continuing training and drills. Those are the activities that expose the shortcomings of a plan. Those are the opportunities for the joint exercises that build relationships and that embed the ability to respond into the DNA of the organization. When the plan is executed, you also must have a process that captures what you did and how well you did so you can revise and improve the plan to do even better next time.

What I wanted to do today was not to create your business continuity plan for you, but rather to say what it is that you should be doing. It is what you should be doing not only to be able to respond in the uncertain event, but also to be able to do a better job of understanding and running your organization effectively and efficiently every day. I think that if you do a good plan, that is what the outcome will be. If you can pass the stress test, everything else is really a piece of cake.

BUSINESS CONTINUITY PANEL DISCUSSION

Figure 1 Panel Discussion, from left to right, Morton Downey, Ron Hynes, Jo Strang, Geoerge Chilson, and Greg Hull

MORT DOWNEY:

Let me introduce our panelists, and we will hear from them shortly.

George Chilson is the President of the National Association of Rail Passengers and one of those people who keeps a conscious eye on how that system is doing. I know he is as concerned about the security aspects of it as he is the funding aspects of it.

Greg Hull, from APTA, is someone who lives and breathes and thinks about this issue every day.

Jo Strang is the Deputy Associate Administrator of the FRA, and I know is very much involved in security and safety issues. I worked with her in the department.

Ron Hynes is the Deputy Associate Administrator from FTA and their R&D activities. We know the priority that the department puts on safety and security.

These are the people who are doing the thinking to make it work for us. I am going to ask each of them to give us a quick response to what they believe to be part of a good continuity effort, and then we will open it up for discussion with the audience.

GREG HULL:

Our new era of security and emergency requirements are placing a significant financial burden on all of our transit agencies. Here in the United States, we simply have not seen an appropriate level of funding to support this new era. We have heard about funding that has been provided to date through the DHS, $250 million, not all of which is yet in the hands of the transit agencies. We know that in the aviation industry somewhere on the order of $18 billion has been provided since 9/11. Yet transit transports over 16 times the number of trips than are taken on domestic air travel.

We know we have a significant risk exposure. We know from data available to us that a significant number of acts of aggression and terrorism happen either directly on or around public transportation facilities. We know that we have a very critical role to play as one of the nation's critical infrastructures. We have a long way to go yet, but certainly through APTA, we are undertaking significant efforts to address these issues with Congress.

I think since 9/11, a lot of our transit agencies have been very effective in the areas of security with respect to prevention, detection, mitigation, and response. But I think we still have a fair bit of work to do on continuity of operations. Our role as a critical infrastructure and a first responder requires transit to be able to resume and maintain services.

Mike Brown, the Chief Operating Officer for the London Underground, came to Washington to provide testimony before the Senate Committee on Homeland Security. He told me about the compelling need for the London Underground to get up and running, and to be seen to be up and running quickly. It was critical, not just for the sake of the public sense of safety and security, but from a financial perspective. They were losing thousands of British pounds every day. With the impact of those events of July 7 and July 21 on them, they needed to address their operations as effectively as they could.

We have had lessons to learn by in the past. We had earthquake situations on the West Coast. We had hurricanes in Florida; Hurricanes Katrina and Rita on the Gulf Coast are

very current lessons to learn by. We had power blackouts in 2004 all across the Northeastern sector that caused a lot of people to look at their operations and in particular to look at redundancies that we need to build into our systems. But as we look at building redundancies into our systems, we go back to the issue of funding, once again.

From a transit management perspective, we need to address a whole number of issues. We have heard that we need to establish mutual aid agreements and certainly to maintain continuity of operations.

There is going to be competition for resources—fuel, energy, electricity—and we need to be diligent about that. We need to develop mutual aid agreements with other transit agencies or other transportation services providers to be able to draw upon them. Those might include school bus operations in your vicinity. It becomes very important as you develop all of those agreements, whether it is with police, fire, et cetera, that you really need to make a great personal effort to establish face-to-face contact. When things hit the fan and you are picking up the phone looking for support, you need to be able to make that connection with the person with whom you had previous contact.

There is a need to identify procedures that can maintain operations when key functions might be lost. For a rail system, that could be when the signals, power switches, or communications systems go down, or when the power to the pumps is lost, whether they are fuel pumps or water pumps. During the Northeast corridor blackout, we heard accounts from a number of agencies where they were able to use generators to power their pumps. Some had made plans to have locomotives that could serve as generators to provide power. Other systems had generators that had not been tested, or tested regularly, and when they went to fire them up, they did not work. So, it is not just a matter of insuring that you have the redundancies, the backup, you also must test them regularly as well.

We heard about communications. You need to determine alternate and multiple ways to communicate with employees. You obviously are going to need to draw upon your employees to provide the services you need to operate the vehicles and provide the maintenance functions. You need to weave the unions into that plan long beforehand. As well, you need to provide for your employees when it comes to their families. If you have employees that are on site, you need to determine how to get word to their families that the person working for you is safe and sound. Similarly, your employees need to know that their families are okay.

Addressing communications with the general public to inform them of services available, you need to use the media, public service announcements, your websites, and having your

employees informed so that if anybody might asks questions of them, they know what is going on. In London during the terrorist attacks, London Transport undertook an outreach to all of the major businesses so those businesses could communicate to their employees as to the availability of services.

We heard that we need to clearly delineate and confirm the understanding of front line people to be able to make decisions and to insure that they know that they are empowered to make decisions at that level.

You need appropriate supplies and emergency supplies, of course, but also, depending upon the circumstances, you may need to decontaminate. How do you do that? Who is going to do that, and, if you do that, who determines when it is safe to operate?

We heard the important role of our accountants. Certainly you need an accountant to track the cost for potential reimbursements and to make payroll. You need to assign a position to document all of the events and activities. You need to recreate a sense of safety and normalcy to your operations.

There are resources available to you, which you can find through the Internet.

Several years ago, the industry, in partnership with the FTA, developed threat-level guidelines to coincide with the Homeland Security's threat levels. There is a level above red called the Purple Level; that is the recovery level and it includes some basic things you can do toward recovery.

There are resources available to you through NFPA 1600. There is a national preparedness standard for private sector preparedness and it includes a portion of business continuity. There is a study available through the National Academy of Sciences, specifically through the Transit Cooperative Research Program (TCRP), on continuity of operations. I encourage you to look for that <http://www.tcrponline.org>.

The FTA is engaged in working with the industry and with APTA on a tool for transit agencies to use that is a web-based ability to conduct tabletop exercises.

Lastly, APTA has become a standards development organization. We have a lot of technical standards for rail, bus, and commuter rail operations, and we are starting to develop standards for security issues. We are partnering with the DHS, TSA, FTA and the FRA on those standards and we look forward to that. If you have ideas that you would like to see incorporated into the development of those standards, please let us know because we need that support.

MORT DOWNEY:

Let me ask you one question before we go on. Are you aware of any formal mutual-aid agreements in the industry that would bring agencies together to share resources?

GREG HULL:

Actually, there are quite a number of such agreements in place. I think most of the major transit systems in the U.S. have such agreements. Those that have them are refining them as time goes by. When 9/11 occurred, WMATA found that it was being included in the plans of other entities that they did not know were mentioning them as a resource. What we are learning as time goes by is the communication and common planning. I believe you could approach any of the major transit systems, whether it is WMATA in Washington, MTA in New York, or BART in San Francisco, and you would find such templates.

MORT DOWNEY:

I also know that if you look at the continuity plans of private employers in any given region, their first item is they are looking for support to get their people to work. I think that is a way we can begin to knit together some mutual support to make the plans more robust.

GEORGE CHILSON:

I am going to approach my remarks from a totally different standpoint. I do not know about you, but if I were sitting in your shoes, I would feel a little bit overwhelmed at this point. You have five years of work to do in the next three weeks. It is not a simple solution, so I am going to try to give you the perspective of your customers, the people who depend on you for their mobility.

The first thing I am going to look for is transportation. If I am at work and I want to go home, I do not want to have to walk home as people had to do after 9/11. I do not want to have to walk home or be faced with having to try to find a different way to get home as did people after the London bomb attacks when the Underground shut down the entire system for the rest of the day.

Responding to keep your customers and maintain business continuity to me, as a customer, means getting the system back up and running as fast as humanly possible. If some segments cannot run, run the others.

In addition to a lot of planning, in some cases this is going to require entrepreneurship and creativity. To give you an example, when Hurricane Katrina was headed toward New Orleans, Dr. John Bertini called me. He is the chairman of the Galveston Island Transportation Museum & Terminal and the organizer of weekend passenger excursion trains that operate into Galveston and occasionally go to Houston. He offered to provide advice to anybody who wanted it because he had some experience in organizing evacuations. There were no takers that time, but when Hurricane Rita threatened Galveston, he worked with Trinity Rail Express (TRE), Amtrak, and Metro. They operated two evacuation trains for Houston. One went to San Antonio, and the other came here to Dallas-Fort Worth on TRE equipment. That happened because one individual had a creative idea, knew what was possible, and was able to pull the levers and get many different agencies working together. If you are looking for an example of mutual aid type agreements, there is an example of one man who put one together in a very short period of time.

The other example I can offer you is when the Northridge earthquake collapsed the Santa Monica freeway. Caltrans told the governor that it was going to be two to two-and-a-half years before they could get it finished. Fortunately, California law gave the governor the emergency powers to suspend a lot of the bureaucratic requirements that would normally be involved with such a project, and they got it done in 66 days. It required breaking the mold; it required breaking out of bureaucratic thinking, and it required focusing on getting the job done, which was getting that highway back into service.

From a customer standpoint, getting the transit system back into service should be a very urgent and top priority. That is what will get people back on the system and continue business continuity. The last thing you want your discretionary riders to do is to think about a habit that has formed over the years and consider the alternative, which is to drive.

Houston Metro, after the hurricane, had its system up and running 36 hours after the hurricane winds departed. I think if there is anybody here from Houston Metro they should take a bow because that is pretty good advance planning and preparation. It would have been back into service sooner, if it had not been for some downed high tension wires for which they had no responsibility.

The second thing I want as a customer is some sort of sense of security that is not just business as usual, but that somebody is watching out for me. That means security measures that are visible and reassuring, but not threatening. Security, policemen, and bomb sniffing dogs are fine. But when you start getting out the submachine guns, you make me wonder if I am going to be as much in jeopardy as any perpetrator that they are going to try to attack.

Also, I am going to want to have a sense of control over my own situation in the future. That is why some of our discussion was on "See something. Say something.," which gives the passenger some sense of control over what is going to happen to them. If they see something that is threatening, they can take an action on their own that will alleviate their stress. That is an important thing—to give passengers some sense of control and remove the sense of fear and helplessness.

Third, you know that attacking the public psyche will be the media harpies playing on the panic banjo. If you can develop reasonable relations with the press in advance and have some key people that you have educated about the nature of the service, the nature of the threat, the safety of the service, and the confidence that people should have in it, this may go a long way, because most of the media people do not understand the basic safety of a transit operation.

The Victoria Transport Policy Institute issued a report in July 2005 saying that if communities that are transit dependent and transit oriented were to have the same traffic fatality rates as the cities that are auto dependent, the number of fatalities a year in this country would go up by about 2,500. In other words, transit saves a great many lives. In London, for example, about 25 percent of the trips are on transit, representing 20 percent of the passenger miles, and yet transit accounts for less than six percent of the fatalities. Transit is an incredible way to save lives, even though the terrorists want to make us believe that it is dangerous to our existence to use it.

The last point I want to make is do not overreact. Transit is not suitable for airline-style security. If we tried to do that we would defeat the entire purpose of the system, which is to make it convenient, easy to use, and time efficient. If we have to go through all those procedures on transit that we do with an airline, it is not going to work. So if you cannot do it [airport-like security] on a subway, and you cannot do it on a commuter train, then there is absolutely no point in trying to do it on an inter city train. Inter city trains do not have the volume, do not have the threat, and they do not represent the risk. They will not

be as attractive a target to terrorists as the high-density, high-capacity trains that operate in subways and in commuter service.

MORT DOWNEY:

The purpose of being in business is to serve customers, and, therefore, business continuity as a part of customer service is a very useful construct to give us.

JO STRANG:

The Federal Railroad Administration is primarily responsible for railroad safety, and that includes commuter rail. Part of our mission is safety, and we view safety as including security, so we also have a security mission. We do this in two ways. We cooperate with our counterparts at DHS. We do joint projects with them. We also do research and development that has both safety and security applications.

Our strategy is if we cannot prevent, we want to mitigate. So we look at both prevention and mitigation as strategies. As an example, one project that we have on mitigation is a chem/bio decontamination project that we are doing at Pueblo, Colorado, in conjunction with the Technical Support Working Group (TSWG). We want to have non destructive agents that can be used to decontaminate transit property: cars, buses, anything that we can use to help mitigate the situation. We are testing various products and trying to find out what will work in what situations and against what agents. That is one mitigation strategy.

We have not talked about the freight rail side of things today, but hazardous materials releases have killed more people in the United States this year than terrorist events. They are accidents we either need to try to prevent through railroad safety improvements, or to protect and mitigate. We are testing products that can be used to coat tank cars that would prevent small arms fire intrusion but could protect lading in case of a derailment. We also are working with the AAR Tank Car Committee. You can both protect the package and improve safety and security. Those things do not happen in isolation.

Another strategy is improving emergency response communications.

When Mort Downey talked about business continuity strategy, one of the elements was mutual aid agreements. In the case of Dallas Area Rapid Transit (DART), I worked with them as part of the Katrina relief efforts. We tried to use Amtrak to evacuate New Orleans.

They had equipment and personnel and they had agreements with the railroads to do it, but we did not have any preplanning done. We had never done any exercises on evacuation and we could not coordinate the communications piece of it, so we got one train out with approximately 550 people onboard.

I encourage using transit and railroads in your emergency response planning. I think if transit properties have an agreement with the state that they can provide it, plan for it, and have a communications strategy in place, rail is a really good option for evacuations, and not just for security events. I believe Frances Edwards mentioned the number one cause is flooding. We have to evacuate people for natural disasters and for security reasons, so there are a lot of applications for having that type of strategy in place.

For those of you that have to pay for it, you need to have your insurance and liability agreements in place to protect yourself. I was talking to Kathy Waters from DART who said the lawyers had a fit because DART had done all of this. She found out after the fact that they were not covered if someone had an accident. This is a real issue and something for which you must have these agreements in place. They did it without incident; nobody was injured. But having an agreement in place to protect you is very important to consider.

The government is trying to coordinate among its branches better. We are still sorting out "who is on first," and we are trying to do that as fast as we can, but the playing field keeps changing. You may have a contact on an issue and find the next week that they are gone and you do not know their replacement. I am sure that, with the addition of Robert Jamison at TSA, things will get better. He was both acting administrator at the FRA, and deputy administrator at FTA, so he knows the people. Plus, having a former deputy secretary from DOT as the deputy secretary at DHS is helpful.

We need to do the paperwork end of things. We do not have Memorandums of Understanding in place for everything. We have one broad one, but we do not have R&D annexed to that, so right now there are twenty-two different tracking projects going on throughout the government. That is a colossal waste of money. I mean, why duplicate efforts? There is no reason for it. We have to become better at coordinating those things.

I want to find out what matters to you. In the railroad industry, we have well established means of communication. We have committees that we work on together. We have conferences that we hold together. We keep in good communications. Those are the types of things that we do not have with state and local governments and from other people. On Monday, I was speaking at the Chlorine Institute's annual meeting about the future of the tank car. I got to hear from a constituent group that I never do, the shippers. Shippers

matter on the freight side of things. I did not know that I was not hearing from them. Because I was not hearing from them, I did not know what I was missing. Finding out what it is that you do not have is the hardest thing to identify; at least it was for me. But now I know they are out there and they want to talk, and we will talk. We will get that set up.

The last thing I wanted to talk about was on some joint projects that we are doing with the Office of Domestic Preparedness. They have done a fantastic job with their risk assessment tool. They worked with FTA and APTA to do that tool and it is a very good one. We are working with them to expand it to include safety, because safety and security are so related that you cannot separate them. Once we have developed this tool, transit properties will be able to use it in their system safety plans and it can become integrated into their environment. That is something that I think will be beneficial. I know that the efforts that have been put in by the FTA, the FRA, APTA, and by the user community, as well as DHS and the Office of Domestic Preparedness, have gone a long way to help get that type of thing out, but it is not done yet. We have to continue to refine and improve it.

RON HYNES:

I am with the FTA Office of Research. We have an Office of Safety and Emergency Management that does a lot of the security work and emergency preparedness work.

I am going to tell you a little bit about the FTA recovery efforts in Lower Manhattan. After 9/11, the FTA established a Lower Manhattan Recovery Office. It is a regional office just for the recovery effort. If you have been to the site, you can see that it is like a cutaway view of a subway. You can watch the pavement above with the buses in the street traffic, and then below ground are the pipelines, and below that are the PATH trains in a kind of a cross-sectional view. So far, we have put over $4 billion dollars into that effort to try to get PATH and the New York City subways back in service. That Lower Manhattan recovery remains a vital regional office just for that rebuilding effort.

FTA and the Office of Research also funds the Florida University Transportation Centers and Drexler University in doing some transit safety and terrorist avoidance and detection systems. These are far out systems that take years to develop.

Today, we talked about training, training, and more training. One thing the FTA Office of Research does is fund the National Transportation Institute and we also fund the Transit Safety Institute in Oklahoma City. The National Transportation Institute does a lot of

training for hijacking and the "if you see it, report it" kind of training, along with how to mitigate, how to isolate, and how to keep on operating if you do have an event.

Lastly, I am going to talk a little bit about commuter rail. It is a completely different thing—heavy rail. Transit or light rail is contained, often, on a fenced right-of-way. Commuter rail is wide open, and often will go through several different counties maybe with different emergency responders. It is good to train, as we talked about earlier, so that you know people before you meet in the middle of an accident or in the middle of a disaster—that you get to trust each other and know each other's capabilities. That helps you work together.

When we drill and drill and train it costs time and effort, but it pays off in huge dividends. I worked for awhile with the National Transportation Safety Board. In an emergency response effort, you may show up at a commuter rail or heavy rail site and you may have things you cannot see that really influence your mitigation efforts, such as an underground high pressure gas pipeline that is buried six feet below grade. Those six feet can go away quickly when you start emergency evacuation or emergency removal of the equipment. Other things may be three feet underground, such as a fiber optics network, or maybe three fiber optics cables together. If you interrupt those, you can sever a lot of your communications that are vital in disaster situations.

Another thing we find when we have some drills is that sometimes emergency responders call the wrong railroad. They think it is railroad A, and railroad A says they stopped all of their trains, but they are really standing in the middle of railroad B. Those things can cost time and confusion. They also can get people hurt. When you make a few mistakes, somebody can come in and shut the whole system down again and that is not what you want to do. It pays to know a little bit about it and the way to do that is to have training and drills.

We had a situation with emergency generators to operate the control points on a railroad. If the power goes out, emergency generators can keep the batteries charged and keep the signal system running. However, they were not used for a long time and the fuel in the generators got stale. People did not know how to operate them. So when they were really needed, they did not work. It takes time and effort to keep all these systems up and running.

MORT DOWNEY:

Let me ask all of you a question. As we think of the requirements or activities that need to be in place to assure capabilities for business continuity, how much do you think we can depend on the good business sense of people who are running agencies or running operations, and how much of it would have to be done as a formal regulatory process?

GREG HULL:

APTA finds that the best processes are those that are developed in partnerships and are not regulatory in nature. We have seen some very interesting approaches developed in partnership. One is a commuter rail safety management program that is a voluntary program. It engages all the commuter rail systems and it is very effective. On the flip side, we have state safety oversight for fixed-guideway systems within the FTA. From my perspective, I see the program that is voluntary and in a full partnership with the FRA as actually being much more effective in taking systems to a much higher level.

GEORGE CHILSON:

In my opening remarks I mentioned the need for creativity, entrepreneurship and innovation. In that kind of environment, I think a regulatory response, except when establishing a broad structure or outline, would probably be quite counterproductive. It has the force of law and tends to focus one's thinking in particular channels when, in fact, there may be different ways of looking at a problem that would produce a much faster and more productive and cost efficient solution.

JO STRANG:

This is going to sound very unusual coming from somebody whose business it is to write regulations, but I really think a regulatory approach would be too cumbersome and you could not have it fit every need.

What we heard earlier on NIMS is the perfect example of that. How do you do this without having a disastrous consequence that was unintended? The people who wrote that regulation did not intend for it to create the confusion and stress that it created. I have written lots of regulations. You do not ever start out saying, "I really want to screw things

up today." But sometimes that can be the unintended consequence because you cannot do something that broad in a regulatory context.

I also think that from Hurricane Katrina we saw lots of examples of businesses pulling together to help their employees. There is a short-line railroad in Port Danville that has 47 employees, 44 of whom lost their homes. They had to clean up and get back to work and they wanted their people to get back to work, so they brought in trailers and they set up temporary housing for the employees. That is the kind of thing that you see repeated over and over. Businesses are there to make money; they are not there to sit on their hands, so they will do things. If we can plan for it with the right people, or at least get them thinking about it, I think that is probably a better approach.

RON HYNES:

I would like to echo those comments. What we saw in Hurricane Katrina in New Orleans is that the system of government seems to have turned into a blame game. But the local things worked well. People had common sense ideas of what to do. When they had the resources, they used them. Railroads moved in trainloads of fuel to help their competition. Actually, that is how other railroads got fuel. We see that today with employees too. Job banks and things like that going on that are not regulatory in nature. It is good to have the framework and it is good to have the support and training that goes along with it. But when it really comes down to keeping things moving, it is going to be the resourcefulness of the people using the resources that they have.

MORT DOWNEY:

Now we will open it up to questions from the audience.

ROD DIRIDON:

There is a gray area between where NIMS leaves off and business continuity starts. I suppose there should not be any difference at all; there should probably be a kind of a merging. We have some pretty good examples of how you write the SEMS/NIMS plans, but there are not many examples, of how you write a business continuity plan because there are so many different situations. Could you give us some guidance as to how you

merge that smoothly from the emergency response to business continuity? Can you give us an idea of where we might find some examples of quality plans that bridge that gap well?

MORT DOWNEY:

I have a couple of thoughts, but Greg, you go first.

GREG HULL:

I do not have specific examples, but from my perspective, within NIMS, within any incident command system, you are dealing with the response to the incident, the management of the incident. With continuity of the operations, you are looking at the extension to the next phase. I think continuity of operations is one of those areas that we still need to develop more strongly in our industry, and that is why we see some guidance documents being developed. The TCRP effort is one of those to help assist the industry. Stephan Parker of TCRP may want to comment on that particular document.

STEPHAN PARKER:

We have a project that is jointly sponsored by the Transit Cooperative Research Program, the National Cooperative Highways Program, and the state DOTs collectively. It is continuity of operations planning guidelines and it gives us templates. There are lots of examples and there is a resource CD. It is quite comprehensive.

I think somebody else had mentioned earlier the NFPA 1600 continuity of operations guidelines for the private sector. If you are looking for something very concise, that gets to the highlights, and might be more appropriate to show to your board members, this is good.

ROD DIRIDON:

In our research at MTI, we have run across several situations where, unnecessarily, actions were taken in the disaster response process that made it very difficult for them to get business continuity. More destructive disaster response efforts than might have been absolutely necessary led to difficulties. Is there a way of kind of melding disaster response and business continuity plans, maybe even exercising the two plans together?

STEPHAN PARKER:

I think you may be talking about mitigation, which gets short shrift in a lot of the discussions. I do not think it is even one of the 36 items on the capabilities list. They talk about preparedness, response, and recovery, but building in mitigations or design considerations that will speed the recovery aspect is not something that has been looked at traditionally. I know the FTA recently has come out with a system security design guidelines through the Volpe Center. I think "design considerations" is the term that is being used there.

MORT DOWNEY:

Rod, I think your idea of joint exercising the plans is something we really should look at. The combination of emergency response entities under the NIMS program, or some of the businesses who are also affected, should begin to think through how it happens.

I am also struck with the idea that public accounting firms in America certify the books of every company. Part of their opinion letter every year is whether this is or is not a going concern. In the U.K., they have begun to take this to the step of asking, "Is this a concern that will still be going after things happen?" This is not a rigid regulatory approach, but it is a businesslike approach to say, "Yes, these people have thought it through," or if they had not, they would not receive a clean opinion. So, this is another group we should probably bring in, but they will want standards. They will want some idea of what is appropriate, but that is not going to be, we hope, a hard and fast government regulation.

STEPHAN PARKER:

There is another resource that I believe continues to be available through the John A. Volpe Center, which developed a very effective program called Connecting Communities. This was provided in most every region across the country as a two-day workshop that was intended for transit systems. The price of admission was that you had to bring along your fellow first responders to look at your preparedness plans to reconfirm or update your plan. If you did not have a plan, you had to work through the development of a plan. A tool like that perhaps can help to bridge a gap as well.

RON HYNES:

The next phase of those Connecting Communities workshops is being organized through the National Transit Institute.

The issue you talked about, bridging the private sector and the public sector, is something that I saw exercised during TOPOFF 3 recently. It is the first time that the Homeland Security Operations Center had a separate group specifically composed of people from the private sector. Traditionally what happens when we go to an exercise is first you work within your own organization, then you work across the various sister agencies in the same city or county, and then maybe you will work across other counties. It is pretty rare that we actually reach out both to private non government organizations and particularly to the private sector. This is the first time I have seen it in a large scale exercise.

MORT DOWNEY:

It was not in TOPOFF 2 as I recall. Other questions?

BRIAN JENKINS:

While it made sense to consolidate these various agencies of the U.S. government that were concerned with security into the new Department of Homeland Security, are we paying an unintended price for that? Is there an unintended consequence—particularly when it comes to looking at broad issues of continuity, recovery, and resiliency—by separating transportation security and putting it into an entity that regards itself as the security enforcement agency and away from Department of Transportation entities that are concerned with the efficiencies of our transportation systems? In other words, are we depriving ourselves of some creative approaches here by creating an enforcement set of notions from what was our looking at the issues in terms of efficiency and in terms of the economy?

GREG HULL:

Certainly through the years, and particularly in the couple of years immediately following 9/11, the industry had a very strong partnership and working relationship with the Department of Transportation, the FTA and the FRA. Many of the programs that we

subsequently developed following 9/11 we did in day-to-day contact and in full partnership.

Now, we appreciate that with the creation of TSA and the directorates within Homeland Security we are looking at relatively new structures. The challenge for us in the industry is to educate the areas of DHS and TSA as to what we already have in place. Within our industry we have the best body of knowledge relative to our industry security and management. We are, by practice, familiar with the type of relationship we had with the DOT.

Now we need to structure our relationship with DHS and TSA. For the very reasons that we have heard here—areas are redefined, people come and go within the DHS and TSA—it places a real strain on how you create those relationships. We are hoping that we are seeing some signs that rays of sunshine are coming through.

We are hoping that we can be a catalyst, to even help towards some tighter coordination, not just to bring together some various efforts that are happening within DHS, but to bring the various federal partners together. Notwithstanding the MOUs that are being signed, we hope to actually forge these partnerships around actual activities. The standards activity is a good example. Here we have an opportunity to develop security-related standards that are not going to be regulatory; they are going to be voluntary. They are going to be performance based and they will engage all of the federal partners and all of the industry together.

JO STRANG:

We have to do a better job of communicating between agencies, and that is clear. We have some working groups that were established by White House directives that are formal in their set up. We communicate with each other, as with the toxin bio-inhalation risk assessment that we do jointly with DHS, TSA, IAIT and other elements.

When it comes to writing directives, I think having full collaboration is critical. We saw with the Passenger Security Directive that they issued a directive or conflicts with the safety regulation; in fact, it would be against the law for you to do it. Those types of things we have to iron out, because it does not work now. I think APTA's effort on standards is going to go a long way to help make that happen. We cannot do things in isolation or we will end up confusing the operators and having things that do not make sense, costing everybody a lot of time and money in fighting back against things that do not make sense.

GEORGE CHILSON:

Does having the Transportation Security Agency as one agency involved with all transportation make sense to begin with? Or, would it make more sense to break it down into airline security, port security, and railroad security because they are each technically very different entities? Would it make a difference, if that happened, whether those agencies reported to the Secretary of Homeland Security or the Secretary of Transportation? Would you have the same inter agency coordination problems even if they reported to the same secretary?

GREG HULL:

We had some very real concerns. The former deputy of transportation moving over as the deputy of Homeland Security provides us with some inspiration that positive things can happen. We had a meeting with Kip Hawley, the TSA Administrator. He has a background with the Union Pacific Railroad and with the DOT and he has an understanding of our issues. Kip Hawley advised us that by bringing Robert Jamison onboard there will be a new era of emphasis on working with our particular industry. We are seeing all of these as very positive signs as we talk about partnership initiatives, whether it is on standards development or in the area of technology. There are a lot of things to be discussed between the federal government and industry. We see some great opportunity to deal with those issues in a very short time.

MORT DOWNEY:

I think Brian's comment does raise a significant issue. You have not just a difficulty in coordination among agencies, but you truly have a clash of cultures.

The culture of a security agency is to avoid occurrences at all cost. An event that might happen a stone's throw from here, left to the Secret Service's enduring mentality would be that a lockdown is by far the safest way to assure that you do not have an untoward event. That is the culture.

The culture of transportation is that movement is good, delivery is good, and people's ability to travel is good. Somewhere that has to be dealt with. If, as Greg suggests, we now have some crossover people who are willing to have that conversation, maybe they can

achieve coordination, which is usually described as an unnatural act among unconsenting adults.

It has to be approached so that we can find a balance that is essentially risk based and addresses both of the concerns, efficiency, and effectiveness, on both security and transportation. It is not a trivial issue.

NICOLE LEGAULT:

It is interesting to hear the comments today, given that under our Canadian Department of Transportation we have kept the security programs within our department. I think that in the long-term there have been a lot of positives that have come out of that decision.

The Public and Safety Emergency Preparedness Canada (PSEPC) department, that is equivalent somewhat to the DHS, also considers the sources of threat more broadly than DHS, as their programs also address business continuity when it comes to natural disasters, in addition to terrorists or other types of events.

As the Public Safety and Emergency Preparedness Canada department, which was more focused on IT threats and natural disasters when it was created in December 2003, now embarks on adopting some of their security management systems they are looking at establishing a similar alert level to that of DHS, one that is more security focused.

My question to the panelists would be, for example, after London or similar events I know that your system has now been more focused than natural alert levels, how does that affect your business continuity planning? From the different perspectives of the panelists, it would help me as the Transport Canada representative that has to explain to PSEPC some of the concerns that the transportation sectors will have on either the recommended steps that the industry must follow, that PSEPC would ask of them, if they do choose to establish a similar alert system.

GREG HULL:

When the Department of Homeland Security developed its color-coded threat levels, we said, "That is nice, what does that mean?," because it meant nothing to us at that point. We were asking those questions from the industry and the FTA was asking those questions. We determined in a collaborative the partnership that we needed to develop a set of guidelines.

The FTA funded some consulting support and together developed a set of guidelines that not only addressed the particular color-coded threat levels, but took us a couple steps beyond. The guidelines were developed so that a transit system, regardless of its size or complexity, whether it is commuter rail or a small bus operation, could adapt them to its own operations.

When the July 7 bombings occurred at the Yellow threat level, the Secretary of Homeland Security announced the level would be going to Orange for mass transit. Well, all of the transit systems had already advanced themselves to that level immediately upon learning of the events in London. Was that mandated? No, they did it on their own because they felt it was the prudent thing to do.

Now, having announced the threat level going to Orange and sustaining that over a period of time was something that we believe had to be regarded in a very serious manner. Without any continuity of threat to agencies in the United States, we were looking at a very significant impact to the systems here in the amount of thousands of dollars of overtime costs every single day. So, in making those decisions, you certainly want to be attentive to the real threats that would require you to be at that extended level. If there are no threats, then you need to drop it back down immediately.

BRIDGETTE ZAMPERINI:

I think it is important to recognize that the TSA has a very cooperative relationship with the Federal Transit Administration. Also I would like to emphasize the need for patience as we go through this process. We are under some new leadership, and, with Robert Jamison coming on board, we do expect to see some changes.

In the meantime, we have some programs and projects. For example, in cooperation with the FTA, we are hosting a safety and security roundtable that is an opportunity to bring together both safety and security coordinators from some of the nation's largest agencies. We are beginning to deal with both of those issues and trying to define where we sit in terms of the full size of the house. We are here to work cooperatively and we are as a service to you. We appreciate your feedback and hope that you keep it coming.

MORT DOWNEY:

I want to come back to the issue of the Department of Homeland Security. One of the very positive benefits of having a consolidated department is in the research and development area. Everyone cannot be inventing the wheel on many of the common methods, technologies and needs that are out there. The level of research funding and research intelligence that has been amassed there is very important to the country. But it has to be in a way that communicates with people out in the field, as to what are the problems and what are the needs. Hearing today that this is a process that will be underway is a very positive development.

JO STRANG:

The FRA already works very cooperatively with DHS Science and Technology. We are hopeful that when you do your consolidation, we can do the same types of things we do with other government agencies, which is compare what we are doing so that we do not duplicate because research dollars are scarce. We do a lot of projects together and we look forward to continuing to do that.

ROD DIRIDON:

May we have a discussion within the panel to see if there are any conclusions in regard to business continuity? The conclusions might talk about resources that could be provided in terms of either products or training.

MORT DOWNEY:

We have heard a lot about coordination, inter agency activity, funding, and bringing in the private sector. What are the key things that we should be recommending to go forward on? Let me ask my panelists where we might be going.

GEORGE CHILSON:

I would like to start with what I think is the most important one thing that tends to get lost in a lot of these discussions and that is the customer, the people that everybody is here to serve. In many ways, we tend to get distracted by other issues that seem to be very

important. We neglect to focus on the main issue that our business is transporting people safely, reliably, and consistently—making a system that is attractive and reliable for them to use.

It was said earlier that the mentality of security is that the best security is to lock the system down, but that is not really what provides the best transportation. We must balance the relative risks, in light of all of the Monday morning quarterbacking that is likely to go on if a mistake is made. In many of these situations, somebody who makes the right decision never gets praised, but the one who makes the wrong decision is the one that is hung out to dry. Thus it is a risk avoidance type of system. I am not sure that is the one that best serves the needs of your customers or your income line.

GREG HULL:

I would not disagree with you at all; I think that is our very first priority.

As we look at all of the influences around us on a federal level, we also have a very significant challenge to look at how we can collectively, in a true partnership, work collaboratively. Rather than having directives issued to us, and rather than seeing products being sprung on us, with good intent—be they to help advance emergency preparedness, security, or continuity of operations—we need to be consciously working together in a full-blown partnership.

I believe that we also have a very significant ongoing challenge that will never end in terms of education. We need education amongst ourselves and our federal partners so that we can clearly and effectively communicate the needs of our industry. Within our industry we have a challenge for education. At the APTA Annual Meeting we had some sessions on security, and there were a lot of people at the policy level within our industry who still do not know all of the issues relative to emergency preparedness, continuity of operations, and security. So, we have a challenge to ensure that everybody within our industry is working with a common base of information.

JO STRANG:

There are two things. One, I think that future plans have to look at rail. If you have emergency responders, or if you are going to do evacuations, get the things in place that you are going to need. If you need to have legal agreements, start working on legal

agreements. Do the planning and tabletop exercises with your counterparts. They cost money, but they really pay off. It is one immediate next step that is something people should be talking about and doing.

The other thing is that we have to do it cooperatively, because it will not work otherwise. We are all very willing to do it. I know TSA and DHS are willing, and APTA has always been a wonderful partner to us, so we are used to working together. But if there are others that we are not working with, that we need to work with, you need to let us know. What are we missing?

RON HYNES:

Coordination is a continuing effort. As people change, as guidelines change, it is a continual effort to keep on top of what is happening.

Another thing to do is look at the uniqueness of each situation and see how transit, rail transit or bus transit, can help to get people away from harm, out of the city, and what different types of harm those cities might face. For instance, New Orleans is a city that may flood. Other cities are more primed for a terrorist attack than cities in the middle of Kansas. We have cities in earthquake zones. How would their different transportation infrastructures function as a team in a coordinated effort to get people out of harm's way? That review should also include agencies that operate or oversee those types of transit.

MORT DOWNEY:

I think that degree of coordination and cooperation should include both those who are specialized and expert in the unusual—law enforcement, first responders, EMTs, helicopter pilots—and those who do the routine, delivering the service to the customer. The more we can involve everyone in the organization, whether it is the accountant, the public affairs department, or the engineers, we need to ask them to think about what it is that their role will be. They do not walk off the scene when the helicopter pilots arrive. No one brings in an airlifted accountant who is specialized in emergency response. We all are part of that response team. It is part of our accountability.

I hope we can find ways to make it clearer to senior management, to boards of elected officials and to all those who have oversight that they need to provide the resources and the guidance that says everyone has to be involved. We all want to be able to succeed in tough

times. We have to think about what it is we need, what are the tools, what are the processes, and we need to learn that.

Just as the relationship with the customer is the same, whether it is under stress or otherwise, the services that are provided are the same. We need to know from the people who manage those services what are the tools they need to be able to do what is needed in those times.

We need to talk more with the research and development community, in a dialogue of what is feasible in the way of technology and then what is applicable in the way of direct implementation.

When I served on the National Academy study which was commissioned late in 2001, the underlying thought of that was the premise that war with terrorists is asymmetrical warfare. They have a tremendous advantage in that they are small, capable of moving whenever they want to move, and do not need a lot of logistics. They can hit us anytime they want, and we can not find them all of the time.

If you think about what is the advantage of the United States, our technological capabilities have won many wars for us. We need to put them to work in this particular situation, but we need to put them to work in a way that is relevant to the threat that they are addressing. I think that the dialogue with people who actually will have to implement things in the field and who have seen the threat and those who have the understanding of what technology can be brought to bear will be a very important way to develop countermeasures that may not stop the terrorists, but maybe would send them somewhere else.

One other conclusion, depressing as it may be, is that this is not something we can ignore. It is not something that we can deal with on our own schedule. It is something we have to accept as a challenge and not give up as a way of dealing with it. I think education, communication, and development of skills has to be part of that. The more prepared we are, the less threatened we will tend to be.

JEANNE LIN:

Just to emphasize what the panel has talked about, there needs to be a lot more cooperation and collaboration. I think prior to 9/11, we were all in our own little worlds, or at least I was. When you are in research and development, you tend to be in a laboratory type of environment. Now there is much more of an acknowledgement that we have to involve the

users. We have to involve our customers and our folks who really know what is going on out there. We cannot develop things in isolation.

You also have to think about maintenance and operations. While it may be pretty cool to toss technology over the wall, the guys on the other side that catch it may find it too heavy. Also they may not have an education in physics to understand how it works, or know that it costs $20,000 a month and you have to calibrate every day. Those sorts of things are important considerations too.

ROD DIRIDON:

Let me draw this to a conclusion by noting that the Mineta Transportation Institute is pleased to be able to act as the functionary for this meeting. This is the third National Security Symposium that we have sponsored, and we will look forward to doing others in the future as the situation merits.

We especially thank our co sponsors: the American Association of Railroads, the American Association of State Highway and Transportation Officials, the American Public Transit Association, the Federal Railroad Administration, the Federal Transit Administration, the National Association for Railroad Passengers, the National Railroad Passenger Corporation (Amtrak), and the Transportation Security Administration of DHS.

I want to thank each of our presenters today and especially thank Jim Swofford for being the coordinator of this project.

APPENDIX A: BRIAN MICHAEL JENKINS PRESENTATION FILES

The Terrorist Threat to Surface Transportation

Brian Michael Jenkins, Director

National Transportation Security Center
Mineta Transportation Institute

September 29, 2005

Recent Events

- Revelation of plot to contaminate Heathrow express
- Bomb attacks on London Transport
- Terrorist attacks on trains in Russia
- Bomb on Philippines ferry

Since Beginning of 2004

- Three terrorist attacks have killed nearly 300 persons on trains and subways (142 killed so far this year)
- More than 3,000 injured
- Terrorist attacks on buses in Israel killed 50, injured 90

Observations Based Upon Mineta Transportation Institute Research Beginning in 1996

- Case studies
- Distilling lessons learned, identifying best practices
- Chronology of nearly 1,000 terrorist attacks on surface transportation (excluding maritime incidents)

Completed MTI Case Studies

- New York City (MTA)
- Atlanta (during the Olympics)
- Amtrak (derailment of Sunset Limited)
- United Kingdom (25-year IRA terrorist campaign)
- Paris (1995-96 terrorist bombings)
- Tokyo (1995 sarin attack)

On-going MTI Case Studies

- Madrid (2004 bombing)
- Russia (2004 attack on Moscow's Metro and subsequent attacks)
- London (2005 attacks on London Transport)

1

Public Surface Transportation Targets Attractive To Terrorists

- Easy access and escape
- Congregations of strangers guarantee anonymity
- Crowds in contained environments vulnerable to conventional explosives and unconventional weapons
- Attacks cause alarm and great disruption

Terrorists Who Attack Transportation Systems Often Seek Slaughter

- Two-thirds of attacks intended to kill
- 37% result in fatalities (compared to 20-25% of terrorist attacks overall)
- 75% of fatal attacks involve multiple fatalities; 28% involve 10 or more fatalities
- Every attack in past two years intended to kill
- Bombs kill an average of 15-20 persons

Targets of Attacks

- Buses (32%), tourist & school buses (8%) and bus terminals (7%) = 47%
- Subways and trains (26%), stations (12%) and rails (8%) = 46%
- Bridges and tunnels (5%) and other (2%) = 7%

Tactics Used

- Bombings (60%), bombs thrown (4%) = 64%
- Ambushes, armed assaults (11%) = 11%
- Standoff attacks, shots fired (9%) = 9%
- Hostage situations (5%) = 5%
- Mechanical sabotage (5%) = 5%
- Arson (3%), threats (4%) = 7%
- Other (1%) = 1%

Terrorist Threat Analysis Has Focused on People Not Infrastructure

- Jihadists have contemplated attacks on bridges and tunnels (New York 1993, Brooklyn Bridge scheme in 2003) however…
- No terrorist attacks on bridges, tunnels, or roads
- Only five percent of 900 surface transportation attacks involved bridges or tunnels
- Almost all were in on-going conflict zones where smaller bridges have been blown up

Roads are Less a Protection Issue and More a Lifeline Issue

- 9/11 demonstrated importance of surface transportation lifelines in New York
- Vital in large-scale evacuation and delivering emergency personnel and equipment
- Lack of coordination criticized in evacuation of Washington, D.C.
- Problems underscored in recent hurricane evacuation

2

Lessons Learned from Response To IRA Terrorist Campaign

- 25-year campaign of terrorism against surface transportation in England
- In all, 17 persons killed, 200 injured
- During peak from 1991 to 1999, 81 explosive devices, 6,589 bomb threats, 9,430 suspicious objects
- But high volume of activity allowed analysis of modus operandi and formulation of strategy

Lessons Learned from Response To IRA Campaign (Cont'd)

- Security measures worked against terrorists and reduced ordinary crime
- Government provided detailed guidance to private sector and general public to improve awareness and security, and to follow standard procedures
- CCTV effectively used
- Covert tests regularly conducted

Lessons Learned from 1995 Sarin Attack on Tokyo Subways

- Three lines hit, 12 dead, 5,500 ill
- Early indicators missed
- Security measures could not have prevented
- Diagnosis of poison and reaction slow–trains with Sarin kept running
- Rail staff unprepared, untrained; some died
- Most illnesses result of panic–only 1,200 persons were actually exposed
- Emergency response unprepared for C/B

Major Lesson of 9/11 Case Study "Saving City Lifelines"

- Crisis management plans supported by regular tabletop and field exercises are critical

Preliminary Lessons Learned From Madrid – Motivations

- Osama bin Laden propaganda
- ETA inspiration–attempts thwarted in 2003
- Elections?

Preliminary Lessons Learned From Madrid – Terrorist Planning

- Attack planning began in late 2002 or early 2003
- Specific operational planning in 2004
- Locals knew schedules–planned to the minute
- Attacks clearly intended to kill (10 kgs of explosives plus 23 ounces of bolts and nails)
- Trial runs?
- Terrorists did not travel with assembled bombs (in London?)

3

Preliminary Lessons Learned From Madrid – Warnings

- No prior "chatter"
- Terrorist propaganda was a warning
- Publicity surrounding thwarted ETA attacks
- Partially-assembled bomb found day before a possible indicator

Preliminary Observations From London Attacks

- Prior plots involving public transportation, possibly inspired by Madrid
- No prior indicators–cells beneath radar
- CCTV does not deter suicide attackers
- CCTV helped in rapid identification, confirmation of suicide, may have accelerated action by 2nd cell
- Response well done (coordination excellent)
- Random search procedures accepted
- "Shoot-to-kill" policy controversial

Additional Issues Arising in London Attacks

- Reaction time?
- Diagnosis
- Communication failure
- Handling massive amounts of information
- Informing the public
- Getting people home
- Ability of 2nd cell to penetrate heightened security
- Psychological effects of second bombing

The Threat is Real

- Terrorist adversaries think in terms of endless war–long-term planning horizons
- Remain determined to carry out attacks–they are opportunistic
- Until jihadist enterprise completely destroyed, operative presumption must be that attack will occur at some time
- Surface transportation clearly part of terrorist target set

The Threat is Real - II

- Attacks on public surface transportation more likely than attacks on roads and bridges, although terrorists have considered bridges
- Large-scale terrorist attacks (9/11 scale), especially with unconventional weapons, or that result in public transportation shutdowns, could place great burdens on roads and traffic control systems

Transportation Targets Definitely in Jihadist Playbook

- Bridges & tunnels mentioned in 1993 New York plot
- Al Qaeda operative targeted Brooklyn Bridge
- Subways attacked in Paris in 1995 and 1996
- 1997 "Flatbush Plot" to carry out suicide bombing on New York subway
- Subsequent plots to attack transportation targets in Singapore, Manila, Milan; attacks by Islamic militants in Manila and Moscow

4

Transportation Targets (Cont'd)

- Madrid attack seen as great success to be replicated
- 2004 attack on New York subway thwarted
- 2005 attacks on London's subways
- Jihadists show persistence in target sets and practiced tactics

Potential Sources of Terrorist Threat

- Local jihadists operating on their own carry out attack (1997 and 2004 plots, 2005 attacks)
- Local or foreign recruits sent to reconnoiter targets, plan operations (Padilla, Faris)
- Local jihadists attack with assistance from abroad (1993 WTC bombing)
- Foreign teams inserted into the country (9/11)

Some Axioms About Security Against Terrorism

- "Right" level of security is difficult to determine
- Cost-benefit analysis doesn't work
- Burden of security determined more by size and number of targets than by magnitude of threat
- Security against terrorism almost always reactive
- Security by itself does not prevent terrorism
- Security does work–by displacing the risk
- Security measures are more easily increased than reduced

Desirable Attributes of Surface Transportation Security

- Ability to increase and decrease security (flexibility)
- Emphasis on technology rather than personnel
- Preventive possibilities focus on response training and crisis planning

Conclusions

- Threat is real, not easily quantifiable; difficult to determine the "right level of security." Security will be reactive.
- Effective security not only includes deterrent and preventive measures, but also efforts to mitigate casualties, damage, and disruption.
- Deterrence and prevention difficult to achieve given nature of terrorism & inherent vulnerability of public transportation. More attention to measures that mitigate casualties, damage, and rapidly restore service.
- Security measures must be flexible.

Conclusions (Cont'd)

- Crisis management is essential.
- Design-in security and construct transportation systems to discourage attack, facilitate surveillance, mitigate consequences, and contribute to emergency response.
- Advanced planning is essential for effective response to threats and incidents.
- Multi-mode communications are essential. Communication breakdowns common problem.
- Must communicate accurate information to users and public; provide continuing information and assistance to relatives and friends of victims–an extremely difficult task, not always done well.

5

APPENDIX B: JEANNE LIN PRESENTATION FILES

Department of Homeland Security
Science & Technology Directorate

National Transportation Security Summit
RAIL SECURITY

September 29, 2005

Ms. Jeanne Lin
Director, Border and Transportation Security Portfolio

S&T Recognizes its Two Largest Constituents are…

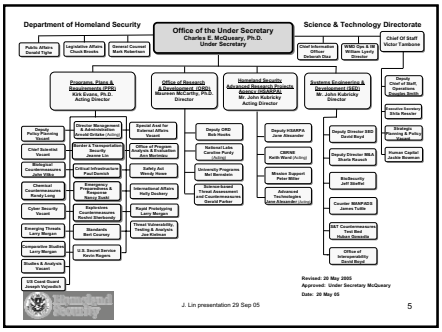
- Border & Transportation Security Forces
  - Customs and Border Protection
  - Immigration and Customs Enforcement
  - Transportation Security Administration
- Federal, State and Local Emergency Services
  - Police, Fire, Emergency Medical Services
  - Emergency Management Agencies
  - City and County Executives
  - FEMA

Rail / Transit Systems

- Inherently open, accessible systems
- 85% of nation's critical infrastructure supporting surface transportation is owned/operated by private sector
- Connection to critical infrastructure – such as airports, seaports, major stations
- Focus on passenger rail/transit systems – mix of subway, light rail and commuter rail
- 11.3 Million passenger trips each weekday on rail/transit systems in 30 cities and 22 states across the nation

DHS Approach

- Leadership and Partnership
  - Future technological developments
- Threat response capability
- Information sharing
- Education and awareness
- Baseline security measures and best practices
- Assessments, plans, exercises
- Funding – state planning process, national priorities
  - UASI Funds: $115 Million in FY03-04 allocated for rail/transit security

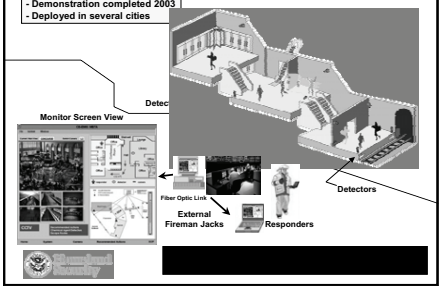


"PROTECT"

- Chemical early-warning system for transit
  - Acronym derives from Program for Response Options and Technology Enhancements for C/b Terrorism
- Commercially available chem detectors and surveillance cameras networked with emergency management info system co-located with metro security command center
  - Autonomous full-time operation, no consumables
  - Initial cost to equip single transit station $250-1000K, depending on complexity
  - Annual maintenance roughly averages $50K per station
- Identified as an allowable expenditure under FY05 ODP Transit Security Grant Program

PROTECT early-warning system for transit

- Demonstration completed 2003
- Deployed in several cities



Rail Security Pilot (Mass Transit)

- Objectives
  - Derive and evaluate an optimal threat-based screening architecture for commuter rail consistent with operational constraints and current technological capability
  - Evaluate promising emerging detection technologies in real commuter rail settings
  - Drive the evolution of explosives countermeasures
- Threat: suicide and leave-behind bombers
  - Explosives and shrapnel
- Targets
  - Human life
  - Rail infrastructure

J. Lin presentation 29 Sep 05 8

Rail Security Pilot Determinations

Using a multi-phased OT&E strategy, we will determine:

- Optimal screening approach for explosives detection in mass transit
  - Vetted concept of operations – evaluated in real stations
  - Optimized and tested training program
  - Detailed list of validated equipment
- Recommendations for announcements for procurement of additional explosives countermeasures and to drive the development of technology toward a solution tailored for the rail environment

J. Lin presentation 29 Sep 05 9

Rail Security Pilot Determinations

(continued)

- Results and recommendations from the evaluation of promising new technology for explosives detection
- Enterprise model that can be used to expand security for all threats to other commuter rail stations and potentially to other transportation hubs

J. Lin presentation 29 Sep 05 10

Border and Transportation Security Portfolio Strategy

- Conduct studies and analysis where needed
- Utilize capabilities where existing or planned
- Insert technology into existing programs (i.e., cargo security)
- Create new capability, if called for (e.g., FAMs)
- Work with customers in a collaborative and cooperative environment
- Involve industry, government, academia
- Develop a systems model for overall view
- Act as a systems integrator

J. Lin presentation 29 Sep 05 11

Capabilities-based Planning

J. Lin presentation 29 Sep 05 12

Capabilities-based Planning Process

Requirements development begins with users:

- Border and Transportation Security operator workshops
  - Conducted eight workshops (general and specific) in two years
  - High-priority capability gaps articulated by front-line officers
  - Vetted by senior management

How do we develop Rail Security requirements?

Capabilities-based Planning Process

Addressing capability gaps & prioritization – inputs/sources

- Public law, policy guidance
- Strategic technology planning process examples
  - Bottom-up (operator) input; top-down (management) validation
  - Technology workshops (capability gaps only)
  - Gaming scenarios
- Customer input and collaboration examples
  - Cargo security, Federal Air Marshals, America's Shield Initiative
- S&T Requirements Council: component input, risk assessments, intergovernmental (DOD, NASA, DOJ, FAA)
- International Collaboration (US/Canada PSTP)

Portfolio Priorities Match Constituents' Priorities

Highest priority requirements are translated into programs

- Border and Transportation Security Portfolio
  - Sensor fusion
  - Real-time access to law enforcement databases
  - Situational awareness
  - Cargo security
- Multiple portfolio requirements
  - Personal protective equipment
- Integrating component and threat requirements
  - Automated scene understanding

Contact Information

Ms. Jeanne W. Lin, Director
Border and Transportation Security Portfolio

Department of Homeland Security
Science & Technology Directorate
Plans. Programs and Requirements

jeanne.lin@dhs.gov

(202) 254-5737

Homeland Security

APPENDIX C: DR. FRANCES EDWARDS PRESENTATION FILES

Why NIMS? Why Now?

Frances L. Edwards, Ph.D., CEM

National Transportation Security Center
Mineta Transportation Institute

Terrorism and Preparedness

- The tragedy of 9/11: Research found
  - Transit was a principal victim
    - NY Subways, PATH
  - More transit and transportation workers were at the WTC site during the recovery than any other profession

Terrorism and Preparedness

- Role of DOT on 9/11
  - Sec. Mineta ordered all planes out of the sky, preventing more carnage
- Homeland Security Presidential Directives
  - HSPD-1 created the Department of Homeland Security
  - HSPD-5 created NIMS
  - HSPD-8 new level of preparedness and coordination across states and professions

HSPD-1

- Created the Department of Homeland Security out of many agencies
- Focus is prevention of terrorism and response to terrorism
- Major entities are FEMA, the Secret Service, the Coast Guard, and recently added a Preparedness Directorate, a medical officer and a cyber-terrorism branch

HSPD-5

- Issued February 28, 2003
- "Management of Domestic Incidents"
- Relevant elements
  - (3) "single comprehensive approach to domestic incident management"
  - (6) "initial responsibility…state and local"
  - (7) "private and non-governmental coordination"
  - (15) "Secretary shall develop National Incident Management System"
  - (16) "Secretary shall develop…National Response Plan"
  - (17) NRP, using NIMS, is "structure…for Federal support to local incident managers"

HSPD-8

- Issued December 17, 2003
- (2)(d) "first responder…those who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment… (including) public works and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response and recovery operations."
- 9/11 proves that transit and transportation are in the forefront of these efforts!

1

HSPD-8 and Transit/Transportation

- Transit as victim of IEDs, suicide bombers
- Equipment for evacuation of threatened areas
  - Rail, light rail, buses, paratransit
- Buses as temporary shelters for victims
- Buses as emergency transportation for disabled, elderly, poor
- Buses as expedient medical transportation for the "walking wounded" from a scene
- Recovery workers: heavy equipment, welders, iron workers, engineers, damage assessment

Lessons of Moscow, London and Madrid

- Transit as victim
  - Israeli and British experiences historically
  - 9/11
  - Moscow subway
  - Madrid commuter rail
  - London subways/bus
- Transit role in response/apprehension
  - Security cameras identified London bombers

Lessons of Moscow, London and Madrid

- Transit role in prevention
  - Security personnel, remove trash bins, change vending machines
- Bringing in the public as a partner in surveillance

HSPD-8 and Transit

- April 27, 2005 National Preparedness Guidance
  - National Preparedness Goal
  - National Planning Scenarios (15)
  - Target Capabilities List (initially 36)
  - Universal Task List (1600 items)
  - "Focus on the capabilities collectively needed to prevent, protect against, respond to and recover from a terrorist attack or natural disaster"
  - "Identify core capabilities…and therefore will drive *how we prioritize our Federal investments*."
  - OVERARCHING NATIONAL PRIORITIES:

#1 = NIMS!

NIMS

- Command and Control
  - Incident Command System in the field
- Resource management, including mutual aid
- Emergency Operations Plans
- "Jurisdictions receiving Federal funds …incorporate NIMS"!

FY 2005 Transit Security Grant Program

- September 8, 2004 letter to governors on NIMS implementation mandates
- All FY 2005 federal preparedness assistance programs begin addressing NIMS implementation
- Transit systems' direction for FY 2005
  - Personnel complete NIMS Awareness course – IS 700 on line
  - Formally adopt NIMS by resolution
  - Evaluate existing compliance – ICS, mutual aid
  - Institutionalize ICS, mutual aid across response system

FY 2006 and FY 2007

- IN ORDER TO RECEIVE 2006 FUNDING, 2005 MINIMUM COMPLIANCE MUST BE MET!
  - Applicants will be required to *certify* that they have met the FY 2005 requirements in their grant application
- FY 2007 NIMS COMPLIANCE IS REQUIRED FOR GRANTS

Who Needs to Take IS-700?

- NIMS Integration Center directive of March 4, 2005 urged that "all personnel with a direct role in preparedness, incident management or response" should take NIMS by October 1, 2005
- FULL NIMS COMPLIANCE BY OCTOBER 1, 2006

Who Needs to Take IS-700?

- Executive Level:
  political and government leaders, agency and organization administrators and department heads; Incident Commanders, personnel who work in a Unified Command, Area Command; Command staff, General staff; MACS personnel, senior emergency managers, EOC staff

Who Needs to Take IS-700?

- Managerial Level:
  agency and organization management between executive level and first line supervisors; personnel who are ICS branch directors, Division/Group supervisors, unit leaders, technical specialists, strike team and task force leaders, single resource and field supervisors, anyone who needs a higher level of ICS/NIMS training to perform in an emergency

Who Needs to Take IS-700?

- Responder Level:
  emergency response providers and disaster workers, entry level to managerial level including EMS, fire, medical, law, public health, public works/utility and other emergency management response personnel
- WHO WILL RESPOND TO AN EMERGENCY IN YOUR ORGANIZATION?

National Preparedness Goal

- Requires state and local entities to achieve and sustain nationally accepted risk-based target levels of capability for prevention, preparedness, response and recovery
- Targets are based on
  - 15 National Planning Scenarios
  - Target Capabilities list (36), includes performance metrics
  - Universal Task List (1600 items)
    - Quantifiable performance measures for planning, training and exercises

3

Resources

- Details on the plans and requirements are at www.dhs.gov
- Planning scenarios, UTL and TCL are at the secure portal – registration required: https://odp.esportals.com
- NIMS updates are at Http://www.fema.gov/nims
- IS-700 is at http://training.fema.gov/EMIWeb/IS/is700.asp

Key Elements of National Systems

- Planning
  - NIMS-compliant EOP
- Operations
  - Alert Level changes
- Equipping
  - Appropriate for prevention, protection, interoperability, recovery

Key Elements of National Systems

- Training
  - NIMS, ICS 100-200, AWR-160
  - Integration with law, fire, EMS
  - Local specific concerns
    - Suicide bomber, IEDs
- Exercises
  - Tabletop, facilitated, full scale
  - BRING TOGETHER YOUR FIRST RESPONDERS!

NIMS Compliance Help from Mineta Transportation Institute

- Research reports on-line http://transweb.sjsu.edu/pubs.htm
  - Jenkins studies of European and Israeli experiences
  - Jenkins and Gerston Bay Area agencies
  - Jenkins and Edwards 9/11 impacts
- Plan writing guidance
  - ICS-compliant plans
- Planning assistance
  - How will you comply with the NRP?
- Preparation of Federally-required documents
- Training assistance
  - Who needs training?
  - In what courses?

NIMS Compliance Help from Mineta Transportation Institute

- Exercise programs
  - Tabletops for executive management
  - Drills for field level skills
  - Facilitated exercises for first responders
  - Functional exercises for operations center staff

QUESTIONS?

4

APPENDIX D: MORTIMER L. DOWNEY PRESENTATION FILES

Mineta Transportation Institute

National Transportation Security Summit

Rail Security

September 29, 2005

Business Continuity Management

Mortimer L. Downey
Chairman, PB Consult, Inc

Business Continuity Management

- This is a timely event and an opportunity to reflect on our readiness
  - Hurricanes
  - London Bombings
  - Anniversary of September 11th

Business Continuity Management

- Business Continuity Management Means What It Says
- The ability to provide appropriate service before, during and after a calamitous event.

Business Continuity Management

- Resilience as a Key Management Advantage
  - Dr Yossi Sheffi "The Resilient Enterprise"

Business Continuity Management

- Crisis Is Not An Everyday Event
- But Preparation for Crisis Is
- And It Can Support Everyday Success

Business Continuity Management

- Business Continuity in the Emergency Cycle
  - Preparation and Mitigation
  - Response
  - Recovery

Business Continuity Management

- Priority for Recovery
  - Low for Others
  - High for You

Business Continuity Management

- Planning is Critical
  - "Proper Planning Prevents Poor Performance"–U.S. Coast Guard

Business Continuity Management

- Key Elements of Successful Planning Process
  - Responsibility Runs to the Top
  - Training and Exercise are Supported
  - Continuity Becomes Part of the Culture
  - Success is Recognized

Business Continuity Management

- Thinking about Continuity
  - A Lot Of It Is the Routine of the Organization
  - And Some of It is Far from Routine

Business Continuity Management

- Key Factors in the Planning Effort
  - Risk Assessment—where should I concentrate my efforts
  - Worst Case Scenarios–Better safe than sorry
  - Understanding Your Business–who better than your managers?

2

Business Continuity Management

- Key Factors in the Planning Effort
  - Building Your Relationships–Who are your partners?
  - Establishing Your Priorities–Keep safety first

Business Continuity Management

- Elements of a Successful Plan
  - Nature of the Plan—simple, understandable, well distributed, frequently updated
  - Clarity in Assigned Responsibilities—who's in charge here?

Business Continuity Management

- Elements of a Successful Plan
  - Identify Key Facilities—and their backups
  - Staff and Job Assignments—how to contact, who does what, who is trained, who is needed at what time

Business Continuity Management

- Elements of a Successful Plan
  - Information Technology—IT backup is an everyday requirement, and an emergency necessity
  - Records—What do you need to stay in business and where do you find them?

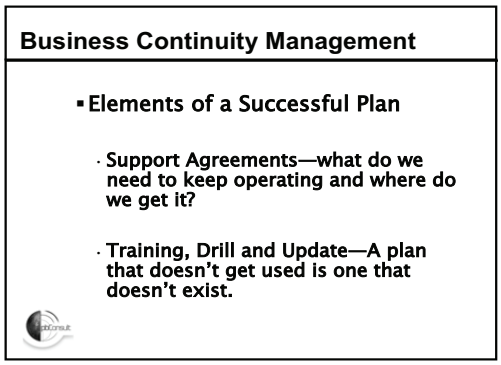
Business Continuity Management

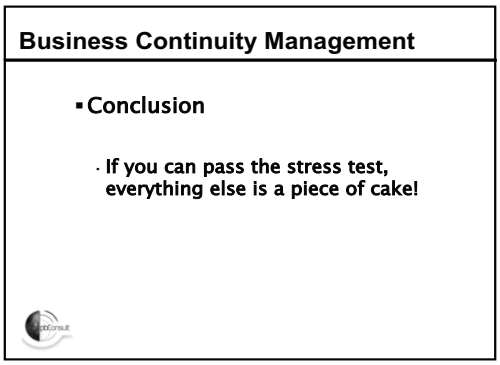
- Elements of a Successful Plan
  - Insurance—Is this an event that insurance will cover
  - Finance--How do we get the cash to operate, and what reimbursement can be obtained?

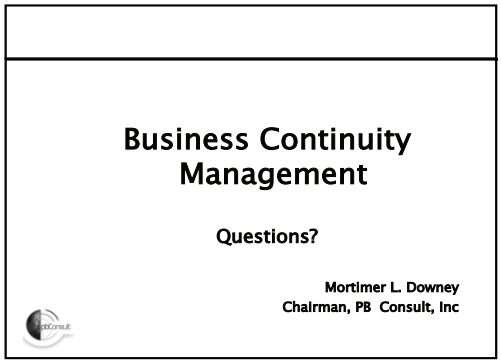
Business Continuity Management

- Elements of a Successful Plan
  - Communications—Who is the spokesperson, will they engender confidence, how do we assure the message

3


Business Continuity Management
Elements of a Successful Plan
Support Agreements—what do we need to keep operating and where do we get it?
Training, Drill and Update—A plan that doesn't get used is one that doesn't exist.


Business Continuity Management
Conclusion
If you can pass the stress test, everything else is a piece of cake!


Business Continuity Management
Questions?
Mortimer L. Downey
Chairman, PB Consult, Inc

4

ABBREVIATIONS AND ACRONYMS

AAR	American Association of Railroads
AASHTO	American Association of State Highway and Transportation Officials
ACE	Altamont Commuter Express
ACLU	American Civil Liberties Union
Amtrak	Pseudonym for the National Rail Passenger Corporation
APTA	American Public Transportation Association
AWR 160	WMD Standardized Awareness Training, Office of Domestic Preparedness
C/B	Chemical/Biological
Caltrain	San Francisco/San José heavy-rail commuter service
CCTV	Closed-circuit television
CDC	Center for Disease Control
Chem/Bio	Chemical/Biological
DART	Dallas Area Rapid Transit
DHS	Department of Homeland Security
DOT	Department of Transportation
EMT	Emergency Medical Technician
EOC	Emergency Operations Center
ESS	Essential systems and services (software)
ETA	Euskadi Ta Askatasuna (Basque separatists)
FAA	Federal Aviation Administration
FEMA	Federal Emergency Management Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
HEPA	High-efficiency particulate air (filter)
HSPD	Homeland Security Presidential Directive
IAIT	Interagency Agreement for Information Technology
ICS	Incident Command System
IED	Improvised explosive device
IRA	Irish Republican Army

MTA	Metropolitan Transportation Authority (of New York)
Metro	Metropolitan Area Transportation Authority (Washington, D.C.)
MIT	Massachusetts Institute of Technology
MOU	Memoranda of understanding
MTI	Mineta Transportation Institute
NFPA	National Fire Protection Association
NIMS	National Incident Management System
NTSC	National Transportation Security Center
ODP	Office for Domestic Preparedness
OSHA	Occupational Safety and Health Administration
PATH	Port Authority Trans-Hudson Corporation, Manhattan/New Jersey heavy-rail rapid transit system
PPE	Personal protective equipment
PROTECT	Program for Response Options and Technology Enhancements for C/B Terrorism
POST	Peace Officers Standards and Training
PSEPC	Public and Safety Emergency Preparedness Canada
PTZ	Pan-tilt-zoom (camera)
R&D	Research and development
Rad/Nuke	Radioactive/Nuclear
S&T	Science and Technology Directorate, Department of Homeland Security
SEMS	Standardized Emergency Management System
TCRP	Transit Cooperative Research Program
TOPOFF	Top Officials Exercise, Homeland Security
TRB	Transportation Research Board, a division of the National Research Council of the National Academies (Science, Engineering, & Medicine)
TSA	Transportation Security Administration
UASI	Urban Area Security Initiative
VTA	Valley Transportation Authority of Santa Clara County
WMD	Weapons of Mass Destruction
WMATA	Washington Metropolitan Area Transportation Authority
WTC	World Trade Center

ABOUT MTI AND THE NTSC

Mineta Transportation Institute was created by Congress in 1991 and won designation as a National Center of Excellence in 2002 by the U.S. Department of Transportation's Research and Special Programs Administration.

MTI is guided by a world-class Board of Trustees and provides thee interdependent services:

1. Research in surface transportation policy conducted by over 120 Ph.D.-level research associates certified by the Institute
2. Postgraduate education through an accredited California State University Master of Science in Transportation Management (MSTM) degree and a professional Certificate in Transportation Management
3. Information transfer via public forums and symposia, a publications library and the *TransWeb* Internet site.

The National Transportation Security Center is the most prominent of five MTI transportation policy research areas. NTSC began in 1995 under the direction of Brian Michael Jenkins to conduct research and information dissemination on transportation counter-terrorism efforts.

NTSC has convened two prior national security symposia; the most prominent was the National Transportation Security Summit on October 30, 2001 in Washington, D.C., and the California Transportation Security Summits (held in Southern and Northnern California) in early 2002.

These and other sessions focused on disseminating U.S. DOT security training program information and NTSC research results. MTI/NTSC has published desensitized versions of the following research papers which are available on the MTI website:

- Formal case studies of 14 major terrorist attacks against surface transportation targets in the world since 1990, including a study of the response on 9/11/01 by the transit systems in New York
- Vulnerability assessments of 11 transit agencies and bridges
- Chronology of reported surface transportation terrorist attacks since 1920
- Summary vulnerability checklist for use by local transportation jurisdictions